Assurance report

TimeLog A/S

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers throughout the period from 1 August 2022 to 30 June 2023

October 2023

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of Contents

Section 1: TimeLog A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with TimeLog A/S, 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.

TimeLog A/S uses the following sub-processors, GlobalConnect and Microsoft. This statement does not include control objectives and related controls at TimeLog A/S' subprocessors. Certain control objectives in the description can only be achieved, if the subprocessor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subprocessors.

Some of the control areas, stated in TimeLog A/S' description in Section 3 of their time tracking system 'TimeLog' can only be achieved if the complementary controls with the customer are suitably designed and operationally effective with TimeLog A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary controls.

TimeLog A/S confirms that:

a) The accompanying description, Section 3, fairly presents how TimeLog A/S has processed personal data for data controllers subject to the Regulation throughout the period from 1 August 2022 to 30 June 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how TimeLog A/S' processes and controls were 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, 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 the data processor's TimeLog in the processing of personal data during the period from 1 August 2022 to 30 June 2023.

(iii) Does not omit or distort information relevant to the scope of TimeLog 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 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 throughout the period from 1 August 2022 to 30 June 2023. If relevant controls with subprocessors were operationally effective and data controller has performed the complementary controls, assumed in the design of TimeLog A/S' controls during the period 1 August 2022 to 30 June 2023. 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; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 August 2022 to 30 June 2023.

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.

Frederiksberg, 20 October 2023
TimeLog A/S

Per-Henrik Nielsen
CEO

Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to TimeLog A/S' data processing agreements with customers during the period 1 August 2022 to 30 June 2023

To: TimeLog A/S and their customers

Scope

We were engaged to provide assurance about a) TimeLog A/S' description, Section 3 of TimeLog in accordance with the data processing agreement with costumers as data controllers throughout the period from 1 August 2022 to 30 June 2023 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the description.

TimeLog A/S uses the following subprocessors: GlobalConnect and Microsoft. This statement does not include control objectives and related controls at TimeLog A/S' subprocessors. Certain control objectives in the description can only be achieved if the subprocessor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The Description does not include control activities performed by subprocessor.

Some of the control objectives stated in TimeLog A/S' description in Section 3 of 'TimeLog', can only be achieved if the complementary controls with the customers (or the specific customer) have been appropriately designed and operating effectively with the controls with TimeLog A/S. The report does not include the appropriateness of the design and operational effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

TimeLog A/S' responsibilities

TimeLog A/S is responsible for: preparing the Description and the accompanying statement, Section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and for the design and implementation of operationally effective controls, to achieve the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark.

Grant Thornton is subject to the International Standard on Quality Control (ISQC 1) [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.

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

Auditor's responsibilities

Our responsibility is to express an opinion on TimeLog A/S' Description and on the design and operational 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 TimeLog 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 that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

(a) The Description fairly presents TimeLog as designed and implemented throughout the period from 1 August 2022 to 30 June 2023;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1 August 2022 to 30 June 2023; to obtain reasonable assurance that the control objectives stated in the Description would be obtained if controls with subprocessor were operating effectively and if data controller has designed and implemented the complementary controls, assumed in the design of TimeLog A/S controls during the period from 1 August 2022 to 30 June 2023, and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved and operated effectively throughout the period from 1 August 2022 to 30 June 2023.

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 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, 20 October 2023

Grant Thornton
State Authorised Public Accountants

Jacob Helly Juell-Hansen
State Authorised Public Accountant

Isabella Ørgaard Jensen
Director, CISA

Section 3: TimeLog A/S' description of processing activity for the supply of TimeLog

Introduction

The following description concerns controls related to data protection and personal data with TimeLog. The purpose of the description is to provide information to TimeLog A/S' customers and their stakeholders about the requirements and contents of the data processing agreements with customers.

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 subsupplier of physical security in data centres and infrastructure, from which TimeLog A/S' customers are operated. GlobalConnect is responsible for the physical security, hardware, network, backup, and storage.

Our control objectives, including rules, procedures, and controls

TimeLog is a market leading Professional Service Automation (PSA) software, targeted consulting and advisory companies who aim high and have the ambition to develop their business and optimize internal workflows all the way from the initial contract to the final invoice. For more than 20 years, TimeLog has grown and today it has offices in Denmark (HQ), Sweden and Malaysia.

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 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. 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 comply 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.

GDPR and TimeLog's 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.

Processing of various categories of personal data

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

- To perform the services, described in the contract for the use of TimeLog's software
- 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:

General personal data, which i.e., can include:

- 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

Technical and organisational control measures

TimeLog has implemented the following control measures to ensure compliance with GDPR.

It can be, for example:

- Information security policies
- Guidelines for human resource security
- Asset management, including control of dispensing and returning of assets upon hiring and termination of employees
- Cryptography
- Supplier relationships and/or supervision plan with sub-data processor
- Security incident management
- Ensuring that data processing agreements with sub-data processors are prepared
- Control and update of risk assessment, policies, and procedures
- Ongoing GDPR training of employees
- Control of access based on a work-related need

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 etc., 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. Furthermore, 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 and due to the requirements for having a DPO are not valid for TimeLog's business.

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 authorized 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. TimeLog has a written procedure to ensure this.

Significant changes in the audit period

At the end of the audit period TimeLog has implemented a new subprocessor.

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 is not transmitted to TimeLog in support cases, via tickets etc.

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

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

Our test of the functionality 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 throughout the period from 1 August 2022 to 30 June 2023.

Our statement, does not apply to controls, performed at TimeLog A/S' sub-processors.

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

We 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	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

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

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2.

Articles and points about main areas are written in bold.

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

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Control objective A - Instructions regarding processing of personal data

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

No.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that procedure has been updated within the audit period and is available for employees.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected that Management ensures that personal data are only processed according to instructions.	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 inquired about the procedures for ensuring verification that personal data are not processed against the Regulation or other legislation. We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. We have inquired if the data processor has received instructions of processing of personal data that was considered to be against legislation.	We have been informed, that the data processor has not received any instructions of processing of personal data that was considered to be against legislation, therefore we have not been able to test the effectiveness of the control. 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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure establishment of the agreed safeguards. We have inspected that the procedures have been updated within the audit period. We have, by sample test, inspected that the safeguards agreed on in data processing agreements have been established.	No deviations noted.
B.2	The data processor has performed a risk assessment and based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	We have inspected that the risk assessment performed is up to date and comprises the current processing of personal data. We have, by sample test, inspected that the data processor has implemented the technical measures ensuring an appropriate level of security, consistent with the risk assessment.	No deviations noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed.	No deviations noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inquired into whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.

Control objective B - Technical measures

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

No.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have, by sample test, inspected that access is restricted to the employees' work-related need for access to systems and databases in relation to processing of personal data. We have inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data. We have inspected that access is restricted to the employees' work-related need for a sample of users' access to systems and databases.	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by e-mail.	We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have inspected that technological encryption solutions have been available and active throughout the assurance period. We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by e-mail.	No deviations noted.
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation, technical errors.	We have inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. We have inquired as to how logs are protected against manipulation and technical errors.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	We have inquired into the procedures for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have, by sample test, inspected that documentation exists regarding regular testing of the technical measures. We have inspected that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner.	No deviations noted.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inspected the procedure for changes in information processing facilities and systems. We have, by sample test, inspected documentation that change requests are being managed according to the established 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 inquired into procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected that resigned employees have had their access rights cancelled. We have inspected the procedure for regular review and assessment of access rights. We have inspected, that review and assessment of access rights has been performed within the audit period.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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 that locations in which data is processed have restricted access.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists that Management has reviewed and approved within the past year. We have inspected documentation that the 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 into.	We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have inspected the procedure for onboarding new employees. We have, by sample test, inspected documentation that new employees have been informed about their roles and responsibilities in information security.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	We have inquired about employee's obligation to maintain information security in connection with termination of employment or contract. We have inspected documentation that information security responsibilities and duties that remain valid after termination or change of employment have been defined and communicated. We have, by sample test, inspected if terminated employees have returned their assets.	We have not received documentation indicating that assets have been returned upon termination of employment. No further deviations noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	We have inquired into procedures to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We have, by sample test, inspected that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality for employees resigned or dismissed during the assurance period.	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 procedures for ensuring adequate education and information security training (awareness training) We have inspected that activities to develop and maintain employees' security awareness have been carried out.	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have inspected the assessment of the need for a DPO and ensured that the company has assessed the need for a DPO during the period.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.9	The processor keeps a record of categories of processing activities for each data controller. Management has ensured that the record of categories of processing activities for each controller includes: • Name and contact information of the data processor, the data controller, representatives of the data controller and data protection officers • The categories of processing, carried out on behalf of the individual data controller. • When relevant, information about transfer to third countries or an international organisation, with documentation of adequate guarantees. • Where possible, a general description of technical and organisational security measures. Regularly – and at least annually – an assessment is made of whether the record of categories of processing activities for each controller should be updated.	We have inspected that the categories of processing contain the following information: • the name and contact details of the processor, and the data protection officer • the categories of processing carried out on behalf of each controller • where applicable, transfers of personal data to a third country or an international organisation • where possible, a general description of the technical and organisational security measures. We have inspected that the categories of processing activities have been updated and approved by management during the period.	No deviations noted.

Control objective D - Return and deletion of personal data

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

No.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. We have inspected that the procedures are up to date.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. We have, by sample test, inspected that specific requirements been agreed with respect to the data processor's storage periods and deletion routines.	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 inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. 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 during the assurance period.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. We have inspected that the procedures are up to date.	No deviations noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions. We have, by sample test, inspected that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
F.1	Written procedures exist which include requirements for the data processor when using sub-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 the 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 subprocessors used. We have, by sample test, inspected that documentation exists that the processing of data by the subprocessor is stated in the data processing agreements – or otherwise as approved by the data controller.	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 inspected that formalised procedures are in place for informing the data controller when changing the subprocessors used. We have inspected documentation that the data controller was informed when changing the subprocessors used throughout the assurance period.	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 inspected for existence of signed sub-processing agreements with subprocessors used, which are stated on the data processor's list. We have inspected that sub-processing agreements include requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.
F.5	The data processor has a list of approved sub-data processors.	We have inspected that the processor has a complete and updated list of subprocessors used and approved.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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 documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment. We have inspected documentation that technical and organisational measures, security of processing at the subprocessors used, third countries' bases of transfer and similar matters are appropriately followed up on.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*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 inquired into the procedures 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 the procedure has been updated within the audit period.	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 inquired into how the transfers to third countries are managed. We have inspected the data processing agreement.	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.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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 that there is valid basis of transfer in place for transfer of personal data to third countries.	No deviations noted.

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

Control objective I – Managing personal data breaches

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

No.	*TimeLog A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedure is in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that the procedure has been updated within the audit period.	No deviations noted.
I.2	The data processor has established controls for identification of possible personal data breaches.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. We have inspected documentation that monitoring alarms, unusual log activities etcetera, are followed up on. We have inspected documentation that logging of access to personal data, is in place.	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 that the data processor has a list of security incidents including whether the individual incidents involved a personal data breach. We have inquired into whether there have been any personal data breaches in the audit period.	We have been informed that there have not been any personal data breaches during the audit period. Therefore, we cannot test the effectiveness of the control. No deviations noted.

Control objective I – Managing personal data breaches

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

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