INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT FOR THE PERIOD FROM 1 JULY 2023 TO 30 JUNE 2024 ON THE DESCRIPTION OF TIMELOG A/S' SERVICES AND THE RELATED CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

TIMELOG A/S

CONTENTS

1. AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT FOR THE PERIOD FROM 1 JULY 2023 TO 30 JUNE 2024 ON THE DESCRIPTION OF SERVICES AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

To: The Management in TimeLog A/S
TimeLog A/S' customers and their auditors

Scope

We have been engaged to report on TimeLog (the service provider) description in section 3 of TimeLog A/S' services and related controls, and on the design and operating effectiveness of controls related to the control objectives stated in the description, throughout the period from 1 July 2023 to 30 June 2024.

The Service Provider's Responsibilities

The service provider is responsible for preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and the statement.

The service provider is responsible for providing the services covered by the description; stating the control objectives; and identifying the risks threatening achievement of the control objectives; designing and implementing effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Assurance

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret revisionsaktieselskab applies International Standard on Quality Management, ISQM 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's Responsibilities

Our responsibility is, on the basis of our actions, to express a conclusion about the service provider's description as well as about the design and operational efficiency of controls related to the control objectives set out in this description.

We have performed our work in accordance with the International Standard on Assurance Engagements 3402 on declaration duties with security checks at a service organisation. This standard requires that we plan and carry out our actions in order to obtain a high degree of certainty as to whether the description is correct in all material respects and whether the controls in all essential respects are appropriately designed and have operated effectively.

A declaration task with certainty to provide a statement about the description, design, and operational effectiveness of controls at a service provider includes performing actions to obtain evidence of the information in the service provider's description as well as of the controls' design and operational effectiveness. The actions chosen depends on the assessment of the service provider's auditor, including the assessment of the risks

that the description is not accurate and that the controls are not appropriately designed or do not operate effectively. Our actions have included tests of the operational effectiveness of such controls, which we consider necessary to provide a high degree of assurance that the control objectives set out in the description were achieved. A statement of assurance with certainty of this type further includes an assessment of the overall presentation of the description, the appropriateness of the control objectives set out therein and the appropriateness of the criteria specified and described by the service provider in section 2.

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

Limitations of Controls at a Service Organisation

The service organiations' description is prepared to meet the common needs of a wide range of customers and their auditors and may not, therefore, include every aspect of TimeLog A/S' services that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in service providers statement in section 2. In our opinion, in all material respects:

a. The description of TimeLog A/S' services and related controls, as designed and implemented throughout the period from 1 July 2023 to 30 June 2024 is in all material aspects, accurate and

b. The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 July 2023 to 30 June 2024; and

c. The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 July 2023 to 30 June 2024.

Description of Tests of Controls

The specific controls tested, and results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended only for customers, which have used the service providers services, and their auditors who have a sufficient understanding to consider it, along with other information about controls operated by the customer themselves when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 18 September 2024

BDO Statsautoriseret revisionsaktieselskab

Claus Bonde Hansen
Partner, State Authorized Public Accountant

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. TIMELOG A/S STATEMENT

TimeLog is a market leading Professional Services Automation (PSA) software, targeting consulting and advisory companies who aim to develop their business and optimise internal workflows all the way from the initial contract to the final invoice.

Our services cover time tracking, project management, automated project invoicing, resource management, invoicing and finances, customer management, reporting, integrations, and employee management.

TimeLog uses sub-service suppliers. The relevant control objectives and associated controls of these service sub-service suppliers are not included in the accompanying description.

The description has been prepared for TimeLog's customers and their auditors who have a sufficient understanding to consider the services, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.

TimeLog confirms that the accompanying description in section 3 fairly presents controls in relation to services and associated controls throughout the period from 1 July 2023 to 30 June 2024. The criteria used in making this statement were that the accompanying description:

1. Explains the services, and how associated controls were designed and implemented, including explaining:
    - The services provided, regarding the handled groups of transactions, when relevant.
    - The processes in both IT and manual systems that are used to initiate the records and process.
    - How the system handles other significant events and conditions than transactions.
    - Relevant control objectives and controls designed to achieve those objectives.
    - Controls that what we have assumed would be implemented by the user companies with reference to the design of the system and which, if necessary to achieve the control objectives stated in the description, are identified in the description along with the specific control objectives we cannot reach ourselves.
    - Other aspects of our control environment, risk assessment process, information system (including the associated business processes) and communication, control activities and monitoring controls that have been relevant to the processing and reporting of customer transactions.
2. Includes relevant details of changes to the controls relating to the service providers services during the period from 1 July 2023 to 30 June 2024.
3. Does not omit or distort information relevant to the scope of the controls described relating to services considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of services that the individual customer may consider of importance to their special environment.

TimeLog confirms that controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 July 2023 to 30 June 2024. The criteria we used in making this statement were that:

1. The risks that threatened achievement of the control objectives stated in the description were identified.

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

3. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 July 2023 to 30 June 2024.

Copenhagen, 18 September 2024

TimeLog A/S

Per-Henrik Nielsen

Per-Henrik Ole Nielsen
CEO

3. TIMELOG A/S' DESCRIPTION OF SERVICES

GENERAL DESCRIPTION OF TIMELOG A/S

This description is prepared for the purpose of reporting on the IT general controls that TimeLog applies to support and safeguard provision of IT operations to its customers. The description focuses on business-related control objectives and processes implemented to safeguard TimeLog provision of IT operations.

The purpose of the report is to provide TimeLog customers and their auditors with information regarding the requirements of ISAE 3402, which is the international auditing standard for assurance reports on controls at service organisations. In the following, a description of the general information security controls related to TimeLog's services to customers, will be provided.

The scope is exposure of the technical and organisational security measures which have been implemented in connection with the operation of TimeLog. We have reviewed all the commonly accepted information security controls specified in ISO 27002:2017. TimeLog has assessed its compliance with these controls as stated under each control.

DESCRIPTION OF TIMELOG A/S' SERVICES IN CONNECTION WITH OPERATING SAAS SERVICES AND RELATED IT SYSTEMS

TimeLog is a market leading Professional Services Automation (PSA) software, targeting consulting and advisory companies who aim high and have the ambition to develop their business and optimise 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) and Malaysia.

TimeLog's services cover time tracking, project management, automated project invoicing, resource management, invoicing and finances, customer management, reporting, integrations, HR, and employee management. An annual risk assessment is carried out and input for this assessment is obtained from all levels in the Company.

TimeLog uses sub-service suppliers within e-mail service, hosting, operating system, customer service software, and outsourcing services.

RISK MANAGEMENT OF SERVICES

An annual risk assessment is carried out and input for this assessment is obtained from all levels in the Company. The risk assessment is conducted to document TimeLog's risk-based approach for selecting security measures and provides an assessment of all identified risks. The purpose of the risk assessment is to ensure that the procedure and implemented security measures match the risk that occur, both when internal and external factors are taken into consideration.

The steps and methodology of the risk assessment follow the process which is considered part of the ISO/IEC security standard. The residual risk is assessed based on the risk image and the implemented security measures.
In this way it is assessed whether the implemented security measures are adequate or if further action should be taken.

TimeLog has a formal process for management of risks which result in specific action plans. The day-to-day Management of TimeLog decides on the basis of the risk assessment whether an identified risk can be accepted, is to be reduced or whether insurance is required based on selected risks.

This report includes solely controls and control objectives for processes and controls that are managed by TimeLog and, thus, it does not include controls or control objectives that are managed by sub-organisations.

CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR CONTROL IMPLEMENTATION

TimeLog's information security is defined on the basis of the objective to provide dedicated IT outsourcing and high-quality infrastructure solutions, including stability and security.

The determination of criteria and scope of control implementation at TimeLog is based on the ISO 27002:2017 framework for management of information security. The following control areas in ISO 27002 were assessed:

- A.5. Information security policy
- A.6. Organisation of information security
- A.7. Human resource security
- A.8. Asset management
- A.9. Access management
- A.10. Cryptography
- A.11. Physical and environmental security
- A.12. Operations security
- A.13. Communications security
- A.14. Acquisition, development and maintenance of systems
- A.15. Supplier relationships
- A.16. Information security incident management
- A.17. Information security aspects of contingency, disaster recovery and restore management
- A.18. Compliance

Implemented control environment
The implemented controls are based on the services provided by TimeLog to customers and include control areas and control activities within operation and hosting. All of the above areas are described in detail in the following in separate paragraphs, and the described control objectives and controls for those areas in the paragraph on control objectives, controls, tests and result of tests are an integral part of the description.

A.5 Information security policy

TimeLog's information security policy creates the framework for an operational management system which implements guidelines on how to handle information security in TimeLog. Responsibility placement, guidelines, risk management and IT contingency plans are therefore topics that are regulated under this management system.

The information security policy covers all activities, including development, delivery, and services to TimeLog's customers. The information security policy is based on generally accepted methods and policies for information security, including best practice in complying with the principles described in the international ISO/IEC 27002 standard. Furthermore, the policy is based on relevant rules, legal requirements, and guidelines within TimeLog's business area.

The information security policy is provided in connection with employment and all employees are required to ensure they are updated periodically in relation to the information security policy. The policy is approved annually. Finally, TimeLog suppliers/business partners are made familiar with the information security policy when obtaining non-disclosure agreements. The information security policy is reassessed annually by the Management.

A.6 Organisation of information security

TimeLog has implemented controls to ensure a general management of the information security including a delegation of responsibilities and handling of material risks in accordance with the requirements of the Time-Log's Management.

Management's obligations in relation to information security
Management takes an active part in the information security in the organisation. The formal responsibility, including approval of the information security policy, is also that of the CEO.

Coordination of the information security
Activities to safeguard the information security are considered in an organisational quality and allocated to relevant departments.

Placing of responsibility for information security
All areas of responsibility for the information security are described in TimeLog's information security policy which clearly describes where the responsibility is placed in relation to information security and the contingency planning.

Placing of responsibility for data protection
The CEO is always responsible for the data protection. Management has delegated this responsibility to the Chief Technology Officer. The Chief Technology Officer manages together with the Compliance Officer the operational responsibility for complying with personal data protection, internally and in relation to customer data.

Mobile data processing and communication
TimeLog's employee handbook sets out guidelines for use of mobile equipment outside the company. All TimeLog employees with a company smartphone are required to install Microsoft Endpoint Company Portal on their device.

Authentication of users on external connections
All access to our network, is only possible for authorized users. Furthermore, TimeLog has two types of VPN connections and access to servers and desktops are gained with RDP.

Non-approved user equipment
Guest equipment and non-approved equipment, for example mobile phones, can solely be connected to a separate guest network.

A.7 Human resource security

TimeLog has implemented controls to ensure that employees are qualified and conscious of their tasks and responsibilities in relation to information security.
General terms of employment, as well as confidentiality is specified in each employment contract.

Management's responsibility
As regards employees, they commit, at their employment, to comply with the company's policies, including the security policy.

Awareness of information security and data protection, education and training
As regards employees, they are informed of all material changes to applicable policies and relevant procedures. The employees are currently informed of personal data protection, so that there is a constant awareness of how employees manage the work with personally identifiable data, their own as well as the customers' data.

During the first 90 days of employment, the hiring manager and Head of People & Culture and Compliance arrange onboarding meetings with new employees where relevant topics related to their job description is

carried out. All employees receive a general introduction on how TimeLog works with information security, and everyone within TimeLog has access to the organisation's information security policy.

It is mandatory for all TimeLog employees to complete awareness training courses which are assigned every second month. The topics vary and are related to information security and data protection.

Roles and responsibilities
The responsibilities of the employees follow their place in the organisation. The responsibilities of all staff in relation to IT security are described in the information security policy.

Non-disclosure agreements
Confidentiality is part of the employment contracts.

Obligations relating to departures
General employment conditions, including conditions in relation to end of employment, are described in the employee's employment contract. Moreover, there is a formal procedure for departure which must be followed by the immediate manager. Head of People & Culture is the ultimate responsible in this respect.

Return of equipment
All employees are to return all received material when the employment contract ends. This is done through a workflow placed at the People & Culture department.

Closing of access rights
TimeLog's formal offboarding procedures ensure that all rights and physical access are withdrawn when an employment ends. This is done through a workflow placed in the People & Culture department. Accesses are reviewed quarterly.

Sanctions relating to breach of the information security
In addition to common employment law provisions, the employee handbook specifies sanctions. The workplace is subject to TimeLog's security routines which must not be broken. If this happens, it is considered a breach of the employment contract.

A.8 Asset management

TimeLog has implemented controls to ensure achievement and maintenance of suitable protection of the organisation's equipment.

Registration of equipment
Relevant equipment, which is utilised, is registered in TimeLog's service desk system. Moreover, there is an updated list of all authorised, mobile units. Non-utilised equipment is stated on an asset list and updated.

Accepted use of equipment
The employees' use of IT equipment and data is subject to guidelines, defined in TimeLog's information security policy and employee handbook.

Management of portable media
TimeLog has implemented procedures for management of removeable media. These procedures are made available to TimeLog employees.

Procedures for information management
TimeLog has implemented appropriate procedures to protect media containing information against unauthorized access, misuse, or corruption during transportation. TimeLog ensures that all laptops are governed by Microsoft Intune and BitLocker encrypted.

A.9 Access management

TimeLog has implemented controls to ensure that access to systems and data are granted through a documented process in accordance with a relevant work-related need and is closed down when the relevant access is no longer necessary.

Procedure for access control
As a supplement to our security policy, TimeLog has a formal procedure for access management.

Guidelines for use of network services
All user rights, including access to network, drives and applications, are determined on the basis of their function. Company networks are separated physically and/or logically to ensure the correct authorized use.

User creation
TimeLog has procedures for creation and closing down of users which are placed in our service desk system in the form of workflows. This process is activated during on/off-boarding and when employees change position and responsibilities within TimeLog.

Extended rights
All rights are managed on the basis of the employees' roles and are checked regularly. Extension of standard rights follows our formal access management procedure. Furthermore, TimeLog has peer-approval on Microsoft 365 services.

Management of password
TimeLog controls the allocation of secret authentication information through a formal management process. For systems supporting initial one-time passwords, TimeLog does not distribute secret authentication information.

Reassessment of user access rights
All accesses and rights are reviewed periodically and as minimum, twice a year.

User identification and authentication
TimeLog has separate admin profiles for all operational staff on systems where it is technically possible.

A.10 Cryptography

TimeLog uses encryption to secure data and communication. On a case-by-case basis, TimeLog identifies risks and determines if encryption is needed, and if so, how strong an encryption is required to mitigate the risks.

Data traffic
TimeLog has a policy on the use, protection, and lifetime of cryptographic keys on a per system basis which covers SSL and code signing.

A.11 Physical and environment security

TimeLog has implemented controls to ensure that IT equipment is properly protected against unauthorised physical access.

Physical access control
TimeLog premises have access control in the form of a required systems key to ensure that only authorised staff have access. Only TimeLog employees receive a key and a code. If suppliers, consultants, or other external parties are to have access, this is only possible together with authorised personnel.

Safeguarding of offices, premises and facilities
TimeLog premises have access control in the form of a system key to ensure that only authorised staff have access.

Protection against physical external threats
We refer to separate ISAE 3402 reports and ISO 27001 on the description of controls, their design and operating effectiveness relating to GlobalConnect.

Public areas, loading and unloading areas
All areas are only accessible with authorised staff. Entrance doors require a personal key. The unloading area at the ground floor is separated by a door where access key is needed.

A.12 Operations security

TimeLog has implemented controls to ensure that operation of servers and key systems is carried out in a structured and secure manner.

Documented operating procedures
All operating procedures are included in TimeLog's document management system and are available to relevant staff who has a work-related need. They are enforced by DevOps scripts and platforms and reviewed minimum once a year.

Safeguarding of systems documentation
TimeLog keeps the systems documentation centrally in our document management system, which can solely be accessed by authorised staff.

Control of procedures for changes
TimeLog's development procedure follows a uniform process for all development activities, which has been portrayed for audit. The development process is normally part of the larger project process, which safeguards that the right initiatives are launched and includes a high-level change management assessment.

Management of capacity
Monitoring of capacity has been implemented in relation to internet, network, servers, disk space and log files. TimeLog receives reporting from GlocalConnect and Microsoft Azure and other tools, which are used in the planning of purchase of additional capacity. Data from monitoring are registered and evaluated currently.

Backup of information
In order to protect against loss of data, TimeLog has established a backup policy and provided adequate backup facilities to ensure that all essential information and software can be recovered following a disaster or media failure.

Control of malicious code
All registered servers in GlobalConnect infrastructure are updated with approved antivirus software according to Best Practice within the area. When a new server is set up, workflows in GlobalConnect service desk ensure that antivirus is installed. All workstations in TimeLog are updated according to Best Practice with antivirus software.

Use of monitoring systems
TimeLog has implemented internal procedures to ensure that alarms are addressed in order to respond to relevant incidents and act accordingly. All relevant alarms are shown on a big screen within normal working hours and to the on-duty officer during on-duty periods. All alarms are reviewed daily by TimeLog's Team Operations and are reported to customers where relevant.

Incident logging
Incidents are registered in different channels depending upon circumstances. Incidents concerning breach in relation to the processing of personal data are reported directly to the Compliance Officer.

Logging of administrator and operator
System administrators' actions are logged automatically.

Logging of errors
Monitoring has been set up for the purpose of future analysis of errors and incidents.

A.13 Communications security

TimeLog has implemented controls to ensure that operation of material infrastructure components is carried out in a structured and secure manner.

Network controls
TimeLog has written procedures for configuration of firewalls, routers and switches, which are solely carried out by GlobalConnect and since March 2024, Unit-IT.

Security services on the network
Access to TimeLog's systems for our customers only goes through public networks. Access and communication between our servers and the internet go through our centrally managed firewall, where logging has been set up. All incoming network traffic goes through our firewalls. Only approved network traffic is allowed through the firewall.

Policies and procedures for data exchange
Formal transfer policy procedures and controls are in place to protect the transfer of information.

Control of network connections
Networks are limited by the VLAN and Access rules in our Core router/firewall. It is solely approved TimeLog and Unit-IT personnel that can access the different VLANs.

A.14 Acquisition, development and maintenance of systems

TimeLog has implemented controls to ensure that servers and relevant infrastructure components are updated and maintained as necessary and that this is done in a structured process.

Change control
TimeLog controls changes to systems within the development cycle using formal change control procedures.
TimeLog uses Git and pull request approval process (gate).
TimeLog reviews and tests business critical applications to ensure that there is no adverse impact on the organisational operations or security when operating platforms are changed.

Control of technical vulnerabilities
Scanning for updates to systems is done by means of Windows update. Hereafter, TimeLog's formal procedure for patching is followed. In accordance with our service agreement with Unit-It (since March 2024), all patching and all vulnerability scanning fall under their domain.

A.15 Supplier relationships

TimeLog uses GlobalConnect and Unit-IT (since March 2024) as sub-supplier of backup. The service provided by GlobalConnect and Unit-IT includes:

- Backup
- Status update

TimeLog uses Dan Group Alarm as sub-supplier of physical security and monitoring. The service provided by Dan Group Alarm includes:

- Monitoring of the physical location
- On-call services in case of alarm

TimeLog uses Amazon Web Service. The service provided by Amazon Web Services include:

- E-mail service.

TimeLog uses Microsoft. The service provided by Microsoft include:

- Operating systems.

TimeLog uses HubSpot. The service provided by HubSpot include:

- Customer service software.

TimeLog uses Pendo. The service provided by Pendo include:

- In-system support.

Management of security in agreements with third party

If the sub-suppliers are an integral part of our services, we inspect the controls implemented by the supplier by obtaining an ISAE 3402 auditor's report.

In addition, relevant providers and consultants are to sign a non-disclosure agreement and confirm that they are familiar with our security policy.

To the extent that TimeLog's sub-suppliers store or otherwise manage personal data on behalf of TimeLog's customers in the course of the sub-supplier's provision of services to TimeLog, the sub-supplier acts as data processor solely according to instructions from TimeLog and TimeLog's customer. Thus, TimeLog's sub-suppliers commit themselves to take the necessary technical and organisational security measures to ensure that personal data are not accidentally or illegally destroyed, lost, or impaired, and that they are not disclosed to unauthorised parties, misused or otherwise processed in violation of data protection legislation.

A.16 Information security incident management

TimeLog has established controls and guidelines which ensure that incidents are dealt with in time and that there is a follow-up on the incidents.

All incidents, including security incidents, follow our formal Incident Management or Request Fulfilment procedure. These are included in our quality management system and bases in our service desk system.

TimeLog has implemented procedures for documentation of all breaches of the management of personal data. All procedures are available to employees with a functional need.

A.17 Information security aspects of contingency, disaster recovery and restore management

TimeLog has prepared a contingency plan which is updated as required.

Information security integrated in the contingency plan

TimeLog has a formal contingency plan in which information security is incorporated.

Development and implementation of contingency plans which include information security

TimeLog has, together with GlobalConnect, a documented process on how to implement and maintain procedures and controls to ensure that the required level of continuity for information security during an adverse situation is handled.

Responsibilities and guidelines

Roles and responsibilities are defined in the contingency plan.

Contingency plan

TimeLog assesses risks regularly, and the contingency plan is updated to the existing risk exposure at least once a year in connection with Management's review and approval of the security policy. GlobalConnect is informed about the changes and an additional review is done. Changes are posted to TimeLog Tech Nirvana and GlobalConnect's document library for TimeLog.

Testing, maintenance and reassessment of contingency plans
The contingency plan is tested annually to ensure that it is applicable, sufficient, and effective.

A. 18 Compliance with laws and internal policies

Licenses for Microsoft software is controlled through Azure Portal, which helps us determining who has access to the licenses. Purchase of Microsoft licenses are done through Fellow Mind.

The servers are set up according to what role they have. However, the same is that they are all patched completely before they are put into service, and antivirus is installed if applicable. It is ensured that it is Unit-IT alone who does this.

CHANGES DURING THE FROM 1 JULY 2023 TO 30 JUNE 2024.

During the declaration period TimeLog A/S has replaced the sub-service provider Whatfix with Pendo, and added Unit-IT A/S service outsourcing division, which previously was owned by GlobalConnect A/S.

COMPLEMENTARY CONTROLS WITH THE CUSTOMER

The customer is obligated to implement the following technical and organisational security measures and other controls to reach the control objectives and thereby comply with the data protection legislation:

- Administration and periodical review of own user profiles and system resources.
- Own internet connection.
- Maintaining traceability in third-party software managed by the customer.
- Own data.
- Compliance with applicable Service Level Agreement which is available on TimeLog's website.
- Correct setup of roles and privileges on the system administration of the product.
- Password management of API users related to the TimeLog product.

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

Objective and scope

BDO has carried out the work in accordance with ISAE 3402 on assurance engagements relating to controls at a service organisation.

BDO has performed procedures to obtain evidence of the information in TimeLog description of services and the design and the operating effectiveness of these controls. The procedures performed depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's test of the design and operating effectiveness of controls has included the control objectives and related control activities selected by TimeLog, and which are described in the following.

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed and operated effectively throughout the period from 1 July 2023 to 30 June 2024.

Test procedures

Tests of the design of technical and organisational security measures and other controls, the implementation and effectiveness hereof were performed by inquiry, inspection, observation, and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel at TimeLog have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Amazon Web Service within e-mail service, we have from an independent auditor received an SOC 1 report for the period from 1 April 2023 to 31 March 2024 on technical and organisational security measures and other controls.

For the services provided by GlobalConnect A/S within hosting service, we have from an independent auditor received an ISAE 3402 report for the period from 1 January 2023 to 31 December 2023 on technical and organisational security measures and other controls.

For the services provided by Microsoft within operating system, we have from an independent auditor received an SOC 1 report for the period from 1 April 2023 to 31 March 2024 on technical and organisational security measures and other controls.

For the services provided by HubSpot within Customer service software, we have from independent auditor received the SOC 2 for the period from 1 May 2023 to 30 April 2023 on technical and organisational security measures and other controls.

For the services provided by Pendo within in-system support and guide for users, we have from independent auditor received the SOC 2 for the period from 1 January 2023 to 31 December 2023 on technical and organisational security measures and other controls.

For the services provided by Unit IT A/S within outsourcing services division, we have from an independent auditor received an ISAE 3402 report for the period from 1 January 2023 to 31 December 2023 on technical and organisational security measures and other controls.

This sub-service provider's relevant control objectives and related controls are not included in TimeLog A/S' description of services and relevant controls related to operation of TimeLog A/S' Outsourcing Services. Accordingly, we have solely assessed the report and tested the controls at TimeLog A/S' that monitor the operating effectiveness of the sub-service provider's controls.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the conclusions specified on the following pages.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

A.5: Information security policies

Control objectives

- *To provide guidelines for and support information security in accordance with business requirements and relevant laws and regulations.*

Control activity	Test performed by BDO	Result of test
5.1.1 Policies for information security ▶ A set of policies for information security is defined and implemented. ▶ The policy includes a guarantee of assistance and obligation to achieve compliance with relevant requirements, laws and regulations.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has implemented an information security policy and observed that its purpose is to support the service provider's activities by ensuring the stability in the availability of the organisation's information assets, the confidentiality of sensitive data, the integrity of data content and compliance with relevant laws and regulations.	No exceptions noted.
5.1.2 Review of policies for information security ▶ The information security policy is reviewed and updated at least once a year.	We have made inquiries with relevant personnel at the service provider. We have inspected the information security policy has been reviewed during the declaration period. We have inspected the service provider's annual cycle of controls and observed that the information security policy is reviewed annually.	No exceptions noted.

A.6: Organisation of information security and internal organisation

Control objectives

- *To establish a managerial basis to initiate and control the implementation and operation of information security in the organisation.*
- To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.

Control activity	Test performed by BDO	Result of test
6.1.1. Roles and responsibilities ▶ The service provider has a clearly divided organisation in relation to information security and has detailed descriptions of responsibilities and roles for the individual employees.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's contingency plan and observed that the service provider has delegated the responsibilities and roles for information security to individual employees.	No exceptions noted.
6.1.2 Segregation of duties ▶ The conflicting functions and responsibilities of the service provider are segregated, to the extent possible, to reduce the possibility of unauthorised or unintentional use, modification or misuse of data.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has assigned user rights based on a need-to-know basis and restricted access accordingly, and we have observed that this is done to reduce the possibility of unauthorized or unintentional use of data.	No exceptions noted.
6.1.3 Contact with authorities ▶ The service provider keeps up to date with news from authorities.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider stays updated with regulatory authorities, receiving newsletters from the Danish Data Protection Agency.	No exceptions noted.
6.2.1 Mobile device policy ▶ Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.6: Organisation of information security and internal organisation

Control objectives

- *To establish a managerial basis to initiate and control the implementation and operation of information security in the organisation.*
- To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.

Control activity	Test performed by BDO	Result of test
	We have inspected the service provider's mobile device policy and observed that the service provider is managing the risk of using mobile devices.	
6.2.2 Teleworking - Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for teleworking and observed that a VPN must be used for remote access to the service provider's production environment. We have inspected that it is not possible to access the service provider's production environment without using a VPN.	No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organization as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
7.1.1 Screening ▶ Screening of potential employees before hiring in the form of interviews and test cases are established.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for screening and recruiting employees and observed that the service provider is required to perform screening of potential candidates through interviews and skill assessments. By random sampling we have inspected that the service provider has performed screening of new employees by interviewing and testing them with a skills assessment.	No exceptions noted.
7.1.2 Terms and conditions of employment ▶ The contract describes the persons concerned and the organisation's responsibility for information security. ▶ All employees have signed an employment contract containing a provision on professional secrecy. ▶ External suppliers/consultants are subject to a duty of confidentiality when entering into a contract.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's template for employment contracts and observed that employees agree to comply with the employee handbook and the service provider's information security policy. We have inspected the service provider's hiring process and observed that it requires new employees to acknowledge that they have read the service provider's information security policy. By random sampling we have inspected that new employees during the declaration period have acknowledged that they have read and understood the service provider's information security policy.	No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organization as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
	We have inspected the service provider's template for employee contracts and observed that employees agree to confidentiality regarding the service provider's business. By random sampling we have inspected the employment contracts and observed that new employees have signed and acknowledged the terms and conditions in the contracts. We have inspected the template for non-disclosure agreements with external consultants and observed that the external consultants sign to confirm that they will use the confidential information solely for the intended purpose and not for their own benefit. By random sampling we have inspected that external consultants have signed a non-disclosure agreement and observed that they are only permitted to use information from the service provider for the execution of their consulting purposes.	
7.2.1 Management responsibilities - Management ensures that all employees and contractors are informed about and maintain the service provider's requirements for information security.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider's Head of People & Culture and Compliance is responsible for ensuring that new employees have read and understood the service provider's information security policy. By random sampling, we have inspected that new employees during the declaration period have acknowledged that they have read and understood the service provider's information security policy.	No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organization as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
7.2.2 Awareness of education and training in information security ▶ All employees of the organisation are receiving appropriate awareness education and training in accordance with data protection and information security, in continuation of the employment. ▶ An introductory course is held for new employees, including information security. ▶ The organisation conducts ongoing awareness training and quizzes of employees in accordance with information security and handling thereof.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for awareness training and observed that the service provider continuously conducts training for employees regarding information security. We have inspected that the service provider uses training modules and observed that these modules include topics related to information security. We have inspected that the service provider has introductory modules for awareness available and observed that all employees have completed this module.	No exceptions noted.
7.2.3 Disciplinary process ▶ There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's employee instructions and observed that there is a section addressing the potential disciplinary action if an employee commits a breach of information security. Upon inquiry, we have been informed that no employees have been subject to disciplinary action, and therefore, we have not been able to test implementation and effectiveness.	We have noted that the service provider has established an instruction regarding disciplinary action. We have not been able to test the implementation and effectiveness of the control, as there have been no disciplinary action during the declaration period. No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organization as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
7.3.1 Termination or change of employment ▶ The organisation has developed and implemented a procedure for offboarding employees. ▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for offboarding and observed that the service provider has developed a checklist that includes items to ensure that mobile equipment is returned and that confidentiality obligations remain in effect after termination. By random sampling, we have inspected that the service provider has completed the checklist for departing employees, where they have returned their mobile equipment and have been informed that their confidentiality obligations remain in effect after termination of employment.	No exceptions noted.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*
- *To ensure appropriate protection of information that is in proportion to the importance of the information to the organisation.*
- *To prevent unauthorised publication, alteration, removal, or destruction of information stored on media.*

Control activity	Test performed by BDO	Result of test
8.1.1 Inventory of assets ▶ Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's inventory of assets and observed that it is associated with information and information processing facilities. We have observed that the service provider continuously updates the inventory.	No exceptions noted.
8.1.2 Ownership of assets ▶ Each asset used is assigned to an owner.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's inventory of assets and observed that each asset used is assigned to an owner.	No exceptions noted.
8.1.3 Accepted use of assets ▶ The organisation has established rules for acceptable use of assets and information.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's employee instructions and observed that they include guidelines for the use of assets, stating that the service provider's assets are to be used for business purposes only.	No exceptions noted.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*
- *To ensure appropriate protection of information that is in proportion to the importance of the information to the organisation.*
- *To prevent unauthorised publication, alteration, removal, or destruction of information stored on media.*

Control activity	Test performed by BDO	Result of test
8.1.4 Return of assets ▶ In connection with the termination of employment, all employees and external party users are returning handed over assets.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for offboarding and observed that the service provider has developed a checklist with items to ensure that mobile equipment is returned. By random sampling, we have inspected that the service provider has completed the checklist for departing employees, where they have returned their mobile equipment.	No exceptions noted.
8.3.1 Management of removable media ▶ The service provider has developed and implemented a procedure for managing removable media. ▶ The service provider uses encrypted removable media for the storage of personal data.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for management of removable media and observed that rules are in for managing removable media. We have inspected that the service provider uses encryption on removable media.	No exceptions noted.
8.3.2 Disposal of media ▶ The service provider has developed and implemented a procedure for the secure disposal of media where information is stored. ▶ The service provider ensures the secure disposal of media, including media where information is stored, to ensure that stored information cannot be accessed.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for media disposal and observed that the service provider ensures the secure disposal of media.	We have noted that the service provider has established a procedure for media disposal. We have not been able to test the implementation and effectiveness of the control, as there have been no disposal of media during the declaration period. No exceptions noted.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*
- *To ensure appropriate protection of information that is in proportion to the importance of the information to the organisation.*
- *To prevent unauthorised publication, alteration, removal, or destruction of information stored on media.*

Control activity	Test performed by BDO	Result of test
	Upon inquiry, we have been informed that no media have been disposed during the declaration period, and therefore we have not been able to test implementation and effectiveness.	
8.3.3 Physical media during transit - Media containing information are protected against unauthorized access misuse or corruption during transportation.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for physical media during transit and observed that mobile phones must be protected with a PIN code, while laptops must have encryption enabled on all drives and be protected with a password. We have inspected that the service provider enforces passwords on mobile devices and observed that these devices are encrypted.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
9.1.1 Access control policy ▶ Access control policy is set up to manage registrations and de-registrations of user access.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has implemented a policy for access control to manage registration and de-registrations.	No exceptions noted.
9.1.2 Access to networks and network services ▶ The service provider only gives co-workers access to networks and network services that they are authorised to use.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for access to networks and network services and observed that access is granted with the minimum user privileges required, where users only have the rights necessary for their job functions.	No exceptions noted.
9.2.1 User registration and deregistration ▶ The service provider has set up a procedure for registering and deregistering the user in connection with the allocation of access rights.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for user registration and deregistration in connection with the allocation of access rights to users. By random sampling, we have inspected user registration and deregistration and observed that the service provider allocates the access rights to users according to the established procedure.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
9.2.2 User access provisioning ▶ The service provider has established a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider has established a formal user access provisioning process to assign or revoke access rights. By random sampling, we have inspected that assigned and revoked access rights during the declaration period and observed that the service provider revokes and assigns for all user types to all systems and services.	No exceptions noted.
9.2.3 Management of privileged access rights ▶ Privileged user rights are assigned based on work-related needs.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for privileged access rights and observed that such access rights are granted based on a need-to-know principle. We have inspected the users with privileged rights at the service provider and observed that the service provider has a limited number of users with privileged rights, and these users have a work-related need for such access.	No exceptions noted.
9.2.5 Review of user access rights ▶ Users and user rights are reviewed at regular intervals.	We have made inquiries with relevant personnel at the service provider. We have inspected the procedure for review of user access rights and observed that the review should be performed regularly.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
	We have inspected that the service provider has performed review of user access rights during the declaration period.	
9.2.6 Removal or adjustment of access rights ▶ The service provider has established a procedure for the revocation and adjustment of access rights. ▶ The service provider revokes and adjusts access rights when employees leave, and agreements terminate.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has established a procedure for the revocation and adjustment of access rights. By random sampling, we have inspected adjusted and revoked access rights during the declaration period and observed that the service provider adjusts and revokes access rights when employees leave, and agreement terminate.	No exceptions noted.
9.3.1 Use of passwords ▶ The service provider has established requirements for passwords which must be followed by all employees and external consultants.	We have made inquiries with relevant personnel at the service provider. We have inspected the established requirements for passwords and observed that these requirements are enforced for all employees and external consultants.	No exceptions noted.
9.4.1 Information access restriction ▶ Access to information and application system functions have been restricted in accordance with the access control policy.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider delegates access rights according to information and systems based on a work-related need.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
9.4.2 Procedure for secure log-on ▶ The service provider has established logical access control for systems with personal information, including two-factor authentication.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for secure log-on and observed that multi-factor-authentication is required to access the service provider's systems.	No exceptions noted.
9.4.3 Password management system ▶ The service provider has set up password management systems and these are active.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for password and observed that the service provider encourages the employees to use password manager. We have inspected the service provider set up policies for the use of password management systems and observed that these are active.	No exceptions noted.
9.4.4 Use of privileged system programs ▶ Only authorised employees can use system programmes that can bypass system and application controls.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for privileged system access and observed that such rights are granted based on a need-to-have principle, which must be approved by either the CTPO or the Information Security Officer. We have inspected that right to privileged system access have been approved by either the CTPO or the Information Security Officer.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
9.4.5 Access control to program source code ▶ Access to program source code is restricted to relevant users.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has restricted the access to program source code to relevant users.	No exceptions noted.

A.10: Encryption

Control objectives

- *To ensure the correct and efficient use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*

Control activity	Test performed by BDO	Result of test
10.1.1 Policy on the use of cryptographic controls ▶ A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have made inquiries with relevant personnel at the service provider. We have inspected the policy for cryptographic controls and observed that the service provider has encrypted web connections between server and services using HTTPS.	No exceptions noted.
10.1.2 Key Management ▶ A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have made inquiries with relevant personnel at the service provider. We have inspected the policy for keys and observed that keys are automatically renewed every year as soon as they expire. We have inspected the relevant control for administration of keys and observed that SSL keys are updated.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.*
- *To ensure a stable supply to* the service provider*'s locations.*
- *To ensure that there is no unauthorised access to* the service provider's *sites.*

Control activity	Test performed by BDO	Result of test
11.1.1 Physical security perimeter ▶ Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security of facilities and security perimeter. We have inspected relevant security perimeter, to ensure that security measures have been implemented to prevent unauthorised access.	No exceptions noted.
11.1.2 Physical entry control ▶ Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical access control an observed the service provider has established physical entry controls. We have inspected that personal access is protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	No exceptions noted.
11.1.3 Securing offices, rooms, and facilities ▶ Physical security for offices rooms and facilities has been designed and applied.	We have made inquiries with relevant personnel at the service provider. We have inspected the information security policy and observed that physical security has been applied to protect offices, rooms, and facilities.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.*
- *To ensure a stable supply to* the service provider*'s locations.*
- *To ensure that there is no unauthorised access to* the service provider's *sites.*

Control activity	Test performed by BDO	Result of test
11.2.7 Secure disposal or service of IT equipment ▶ The service provider gets IT equipment repaired on-premises and monitors the repair. ▶ The service provider disposes of IT equipment by physical destruction of data-bearing media. ▶ The service provider securely deletes data on data-bearing media. ▶ The service provider keeps a record of destroyed IT equipment.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedures for repair and disposal of IT equipment and observed that an external technician must repair the equipment at the service provider's supervision. We have inspected the service provider's procedures for repair and disposal of IT equipment and observed that during the disposal of IT equipment, either a complete deletion or destruction of the disk is performed. We have inspected the list of destroyed IT equipment and observed that no IT equipment has been destroyed during the declaration period. Therefore, we have not been able to test implementation and efficiency.	We have noted that the service provider has established a procedure for disposal and repair of IT equipment. We have not been able to test the implementation and effectiveness of the control, as there have been no destroyed IT equipment during the declaration period. No exceptions noted.
11.2.8 Unattended user equipment ▶ The service provider has established rules for leaving equipment unattended.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for keeping privacy and observed that employees are advised to not leave equipment unattended.	No exceptions noted.
11.2.9 Policies for tidy desk and blank screen ▶ Screen lock is activated automatically after 5 minutes. ▶ Employees must activate screen lock when leaving the client.	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.*
- *To ensure a stable supply to* the service provider*'s locations.*
- *To ensure that there is no unauthorised access to* the service provider's *sites.*

Control activity	Test performed by BDO	Result of test
	We have inspected the service provider's security baselines and observed that there is an automatic screen lock after five minutes. We have inspected the service provider's privacy policy and observed that employees must lock their screens when leaving equipment unattended.	

A.12: Operational reliability

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
12.1.1 Documented operating procedures ▶ Operating procedures have been developed and made available to relevant employees.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has developed operational procedures and observed that these are available to the relevant employees.	No exceptions noted.
12.1.2 Change management ▶ The service provider has established change management procedures.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's change management procedure and observed that changes are submitted for review and must go through a quality assurance process before being deployed to the production environment. By random sampling we have inspected a selection of changes made and observed that these have been approved, tested, documented and implemented in the production environment, according to the change management procedure.	No exceptions noted.
12.1.3 Capacity management ▶ The se of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's capacity management procedure and observed that the service provider monitors the collected parameters. By random sampling, we have inspected a selection of alerts collected by the service provider from monitoring and observed that the service provider has ensured the system performance is maintained.	No exceptions noted.

A.12: Operational reliability

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
12.1.4 Separation of development, testing and production environment - A functional separation between development and operation has been introduced. - Modifications of functionality are tested before it is put into operation. - Development and testing are performed in development environments that are separate from production systems. - A version control system is used which registers all changes in source code. - Development and test environments are separate.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for development and observed that development and change tasks must be verified before being deployed to the production environment. By random sampling, we have inspected development changes and observed that these have been approved by one or more individuals. We have inspected the service provider's network topology and observed that the service provider has segmented their development environment, test environment, and production environment. We have inspected the service provider's use of a version control system and observed that all changes to the source code are registers.	No exceptions noted.
12.2.1 Control against malware - Controls are implemented for detection, prevention, and recovery to protect against malware, combined with appropriate user awareness.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's information security policy and observed that the service provider continuously monitors that antivirus software is installed and updated. We have inspected the service provider's devices and observed that antivirus software is installed on them.	No exceptions noted.

A.12: Operational reliability		
Control objectives ▶ *To ensure proper and safe operation of information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
12.3.1 Information backup ▶ Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's backup policy and observed that backups of servers are performed daily. We have inspected that daily backups of servers are performed and observed that the service provider regularly tests backups. We have inspected that the service provider has performed restore tests during the declaration period.	No exceptions noted.
12.4.1 Event logging ▶ Event logs recording user activities exceptions faults and information security events shall be produced, kept, and monitored.	We have made inquiries with relevant personnel at the service provider. We have inspected that event logs recording user activities, exceptions, faults, and information security events are generated, retained, and monitored.	No exceptions noted.
12.4.2 Protection of log information ▶ Logging facilities and log information are being protected against tampering and unauthorized access.	We have made inquiries with relevant personnel at the service provider. We have inspected that only users with privileged rights can clear the log and observed that it is not possible to tamper the log.	No exceptions noted.
12.4.3 Administrator and operator log ▶ System administrator and system operator activities have been logged and the logs are protected.	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.12: Operational reliability		
Control objectives ▶ *To ensure proper and safe operation of information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected that administrator activities are logged. We have inspected that the service provider reviews the logs of system administrators and observed that the system administrators cannot edit the logs.	
12.4.4 Clock synchronization ▶ The clocks of all relevant information processing systems within the organisation or security domain have been synchronized to a single reference time source.	We have made inquiries with relevant personnel at the service provider. We have inspected that the domain controller enforces time synchronisation of all connected servers.	No exceptions noted.
12.5.1 Software Installations on operating systems ▶ The service provider has implemented procedures for software installation on operational systems.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider's installation of software on operational systems is performed by the supplier Unit-it A/S. We have inspected that the supplier performs security patches and updates on the service provider's operational systems on a weekly basis.	No exceptions noted.
12.6.1 Management of technical vulnerabilities ▶ Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organization's exposure to such vulnerabilities is evaluated and appropriate measures are taken to address the associated risk.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for vulnerability scanning and observed that vulnerability scans are conducted quarterly by an external party with the results documented in a report.	No exceptions noted.

A.12: Operational reliability

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
	By random sampling, we have inspected that the service provider has identified vulnerabilities in the vulnerability scanning report and observed that the service provider has mitigated these vulnerabilities. We have inspected that the service provider has documented their handling and mitigation of weaknesses found.	
12.6.2 Restrictions on software installation - The service provider has established rules for software installations.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's policy for restrictions on software installation and observed that the service provider has imposed restrictions on software installation for standard users, while developers are exempt because it is necessary for them to be local administrators.	No exceptions noted.

A.13: Communication security		
Control objectives ▶ *To ensure the protection of information in networks and of supporting information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
13.1.1 Network management ▶ The network topology is structured according to best-practice principles, which means that servers that run applications cannot be accessed directly from the Internet. ▶ The service provider uses known network technologies and mechanisms to protect internal network.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's network topology and observed that the servers that run applications cannot be accessed directly from the Internet. We have inspected the service provider's network topology and observed that the service provider uses mechanisms such as firewalls and VPNs to protect the internal network. We have inspected that the service provider's firewall is configured by the supplier GlobalConnect.	No exceptions noted.
13.1.2 Securing network services ▶ The service provider has implemented/required appropriate security measures to protect its network services.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider updates the firewall and software for identifying network vulnerabilities on a weekly basis.	No exceptions noted.
13.1.3 Segregation of networks ▶ The service provider has divided its network so that the systems cannot communicate directly.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's network and observed that the network has been segmented and cannot directly communicate with each other directly.	No exceptions noted.

A.13: Communication security

Control objectives

- *To ensure the protection of information in networks and of supporting information processing facilities.*

Control activity	Test performed by BDO	Result of test
13.2.1 Information transfer policies and procedures ▶ The service provider has implemented procedures and controls to ensure that protected information transfers.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for information transfer and observed that confidential information must be transferred via encrypted transmission and should only be shared with third parties if there is a legitimate reason.	No exceptions noted.
13.2.4 Confidentiality or non-disclosure-agreements ▶ Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information, are identified, and documented.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's template for employee contracts and observed that employees agree to confidentiality regarding the service provider's business. By random sampling we have inspected the employment contracts and observed that new employees have signed and acknowledged the terms and conditions in the contracts. We have inspected the template for non-disclosure agreements with external consultants and observed that the external consultants sign to confirm that they will use the confidential information solely for the intended purpose and not for their own benefit. By random sampling we have inspected that external consultants have signed a non-disclosure agreement and observed that they are only permitted to use information from the service provider for the execution of their consulting purposes.	No exceptions noted.

A.14: Acquisition, development and maintenance of systems

Control objectives

- *To ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems which provide services over public networks.*

Control activity	Test performed by BDO	Result of test
14.2.1 Secure development policy ▶ The service provider has developed procedures and controls for the development of systems and software in the organisation.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's secure development policy and observed that all source code must be stored securely, with access to the source code managed through group policies to ensure that only relevant employees have access. We have inspected that only relevant employees have access to the source code.	No exceptions noted.
14.2.2 Procedure for managing system changes ▶ The service provider has developed procedures for system changes.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's development process and observed that backlog items are pulled, broken into tasks, committed to a feature branch, and after code completion and approval, merged into production with tasks marked as complete. By random sampling we have inspected a selection of changes made and observed that these have been approved, tested, documented and implemented in the production environment, according to the development process.	No exceptions noted.
14.2.3 Technical review of applications after changes to operating platforms ▶ When operating platforms are changed business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's development and change management procedure and observed that all changes are submitted for review and must pass a quality assurance process before being deployed to the production environment.	No exceptions noted.

A.14: Acquisition, development and maintenance of systems		
Control objectives ▶ *To ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems which provide services over public networks.*		
Control activity	**Test performed by BDO**	**Result of test**
	By random sampling we have inspected a selection of changes made and observed that these have been reviewed and passed a quality assurance process before being deployed into the production environment, according to the development and change management procedure.	
14.2.5 Secure system engineering process ▶ Principles for engineering secure systems have been established, documented, maintained and applied to any information system implementation efforts.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has established a procedure for development, policy for secure development and secure development environment and observed that the developers must follow these. By random sampling we have inspected a selection of changes made and observed that the development is according to the procedure for development, policy for secure development and secure development environment.	No exceptions noted.
14.2.6 Secure development environment ▶ There is established appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's policy for secure development environments and observed that developers can set up their own development environments on their personal devices.	No exceptions noted.
14.2.7 Outsourced development ▶ The organisation is supervising and monitoring the activity of outsourced system development.	We have interviewed relevant personnel with the service provider. We have inspected the procedure for outsourced development and observed, that outsourcing partner or consultants must sign a non-disclosure agreement.	No exceptions noted.

A.15: Supplier relations

Control objectives

- *To ensure the protection of the organization's assets to which suppliers have access.*

Control activity	Test performed by BDO	Result of test
15.2.1 Monitoring and review of third-party services ▶ The organisation regularly monitors, review and audit supplier services delivery.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has conducted monitoring of suppliers and observed that the service provider has obtained audit reports from suppliers. We have inspected documentation for monitoring of suppliers and observed that the service provider has addressed the results from the audit reports. We have inspected the Amazon Web Services SOC 1 report for the period 1 April 2023 to 31 March 2024. We have inspected the Microsoft SOC 1 report for the period 1 April 2023 to 31 March 2024. We have inspected Global Connect's ISAE 3402 report for the period 1 January 2023 to 31 December 2023. We have inspected HubSpot's SOC 2 report for the period 1 May 2023 to 30 April 2024 We have inspected Pendo's SOC 2 report for the period 1 January 2023 to 31 December 2023. We have inspected Unit-IT's ISAE 3402 for the period 1 January 2023 to 31 December 2023.	We have inspected that the service provider has not conducted audit of HubSpot. No further exceptions noted.

A.16: Management of information security incidents

Control objectives

- *To ensure a uniform and effective method of managing information security incidents, including communication of security incidents and vulnerabilities.*

Control activity	Test performed by BDO	Result of test
16.1.1 Responsibilities and procedures ▶ Management responsibilities and roles have been established in connection with breaches of personal data security. ▶ The organisation has implemented procedure for breach of personal data security.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's policy for information security incidents and observed that the responsibility for handling information security incidents is established. We have inspected that the service provider has established a set of procedures within their information security incident policy and observed that these procedures cover reporting information security events, initial assessment and triage, detailed investigation, incident classification, and incident response. Upon inquiry we have been informed that no information security breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and effectiveness.	We have noted that the service provider has established a set of procedures regarding information security incidents. We have not been able to test the implementation and effectiveness of the control, as there have been no information security incidents during the declaration period. No exceptions noted.
16.1.2 Reporting of information security incidents ▶ The service provider reports information security incidents to relevant parties.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's policy for information security incidents and observed that the Marketing department is responsible for communicating the incidents to customers via email and on the service provider's website. Upon inquiry we have been informed that no information security breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and effectiveness.	We have noted that the service provider has established a policy for information security incidents. We have not been able to test the implementation and effectiveness of the control, as there have been no information security incidents during the declaration period. No exceptions noted.
16.1.3 Reporting information security vulnerabilities ▶ Employees and contractors using the organization's systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for reporting information security events and observed that all employees are	We have noted that the service provider has established procedure for reporting information security events. We have not been able to test the implementation and effectiveness of the control,

A.16: Management of information security incidents		
Control objectives ▶ *To ensure a uniform and effective method of managing information security incidents, including communication of security incidents and vulnerabilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	required to report suspicious activities and security incidents to the operations team, which is responsible for assessing and investigating the suspicious activity and security incidents. Upon inquiry we have been informed that no information security breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and effectiveness.	as there have been no information security incidents during the declaration period. No exceptions noted.
16.1.4 Assessment and decision on information security incident ▶ Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for initial assessment and triage and observed that the operations team is responsible for assessing the incident. Upon inquiry we have been informed that no information security breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and effectiveness.	We have noted that the service provider has established a procedure for initial assessment and triage. We have not been able to test the implementation and effectiveness of the control, as there have been no information security incidents during the declaration period. No exceptions noted.
16.1.5 Response to information security incidents ▶ The organisation decides on information security breaches in accordance with its procedures.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's policy for information security incidents and observed that after the operations team has assessed and identified the information security incident, immediate decisions must be made to implement measures that mitigate the confirmed incident. Upon inquiry we have been informed that no information security breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and effectiveness.	We have noted that the service provider has established a policy for information security incidents. We have not been able to test the implementation and effectiveness of the control, as there have been no information security incidents during the declaration period. No exceptions noted.

A.17: Information security aspects of emergency, emergency and re-establishment management

Control objectives

- *To ensure a uniform and effective method of managing information security incidents, including communication of security incidents and vulnerabilities.*

Control activity	Test performed by BDO	Result of test
17.1.1 Planning for information security continuity ▶ The service provider has established a contingency plan that ensures rapid response time to restore the availability of and access to personal information in a timely manner in the event of a physical or technical incident.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has established a contingency plan and observed that the service provider has set recovery times for systems. We have inspected the service provider's contingency plan and observed that the service provider has defined the responsibilities for roles that should be contacted in case of an incident.	No exceptions noted.
17.1.2 Implementation of information security continuity ▶ The service provider has implemented controls to ensure the continuity of information security.	We have interviewed relevant personnel with the service provider. We have inspected the service provider’s annual cycle of control and observed that the contingency plan is reviewed annually. We have inspected that the service provider holds Disaster Recovery Meetings in relation with testing the contingency plan.	No exceptions noted.
17.1.3 Verify, review and evaluate information security continuity ▶ The service provider has established periodic testing of the contingency plan in order to ensure that the contingency plans are up-to-date and effective in critical situations. ▶ Contingency tests are documented and evaluated.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has performed test of the contingency plan and observed that this test is documented and evaluated.	No exceptions noted.

A.18: Compliance		
Control objectives ▶ *To prevent violation of legal, regulatory, or contractual requirements in relation to information security and other security requirements.*		
Control activity	**Test performed by BDO**	**Result of test**
18.2.1 Independent review of information security ▶ The service provider performs regular reviews of their policies.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's annual cycle of control and observed that the policies are to be reviewed regularly, on an annual basis. We have inspected a selection of the service provider's policies and observed that they have been updated and reviewed during the declaration period.	No exceptions noted.
18.2.2 Compliance with safety policies and safety standards ▶ The service provider carries out regular reviews of relevant procedures and controls.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's annual cycle of control and observed that the procedures are to be reviewed regularly, on an annual basis. We have inspected a selection of the service provider's procedures and observed that they have been updated and reviewed during the declaration period.	No exceptions noted.
18.2.3 Examination of technical conformity ▶ The service provider conducts a regular review of compliance with the organisation's information security policies and standards.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for technical compliance review and observed that the service provider conducts regular reviews of the systems and services to ensure they comply with the policies and procedures.	No exceptions noted.

5. SUPPLEMENTARY INFORMATION FROM TIMELOG A/S

The supplementary information below has not been the subject of the audit carried out by BDO.

Based on BDO's ascertained exceptions in the ISAE 402 declaration, TimeLog has the following supplementary information:

Control activity	Result of test	Comment of the company
15.2.1 Monitoring and review of third-party services ▶ The organisation regularly monitors, review and audit supplier services delivery.	We have inspected that the service provider has not conducted audit of HubSpot.	We acknowledge the auditor's finding regarding the lack of documentation for the supervision of HubSpot. While we confirm that the supervision was carried out as per our internal procedures during the declaration period, just as all our other sub-service suppliers, including reviewing relevant audit reports and certifications, we did not maintain sufficient documentation to support this activity. Going forward, we will ensure that all supervision activities are properly documented to demonstrate compliance with the control requirements.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk