INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 JULY 2023 TO 30 JUNE 2024 ON THE DESCRIPTION OF TIMELOG A/S' SERVICES AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS RELATED TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

TIMELOG A/S

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 JULY 2023 TO 30 JUNE 2024 ON THE DESCRIPTION OF TIMELOG A/S' SERVICES AND NAME OF THE COMPANY AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS RELATED TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of TimeLog A/S
TimeLog A/S' Customers

Scope

We have been engaged to report on TimeLog A/S' (the Data processor) description in section 3 of TimeLog A/S' services and TimeLog A/S and the related technical and organisational measures and other controls, related to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls related to the control objectives stated in the description for the period 1 July 2023 to 30 June 2024.

The Data processor's Responsibilities

The Data processor is responsible for preparing the statement in section 2 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data processor is responsible for providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Control

We have complied with the 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 to express an opinion on the Data processor's description in section 3 and on the design and operating effectiveness of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed.

An assurance engagement to report on the description, design and operating effectiveness of controls at a Data processor involves performing procedures to obtain evidence about the disclosures in the Data processor's description and about the design and operating effectiveness of the controls. The procedures selected

depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the suitability of the criteria specified by the Data processor and described 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 Data processor

The Data processor's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the use of TimeLog A/S' services and Name of the company, that each individual Controller may consider important in their own environment. Also, because of their nature, controls at a Data processor may not prevent or detect all breaches of the personal data security. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

a. The description presents fairly TimeLog A/S' services and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented for the period 1 July 2023 to 30 June 2024.

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed for the period 1 July 2023 to 30 June 2024.

c. The technical and organisational measures and other 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 Test of Controls

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

Intended Users and Purpose

This report is intended solely for data controllers who have used TimeLog A/S' services, and who have a sufficient understanding to consider it along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

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 A/S processes personal data in relation to TimeLog A/S' services and TImeLog A/S to our customers, who are Data Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used TimeLog A/S' services and TImeLog A/S, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

TImeLog A/S uses sub-processors. These sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

TImeLog A/S confirms that the accompanying description in section 3 fairly presents TimeLog A/S' services and the related technical and organisational measures and other controls for the period 1 July 2023 to 30 June 2024. The criteria used in making this statement were that the accompanying description:

1. Presents TimeLog A/S' services, and how the related technical and organisational measures and other controls were designed and implemented, including:
    - The types of services provided, including the type of personal data processed.
    - The processes in both IT systems and business procedures applied to process personal data and, if necessary, correct and delete personal data as well as limiting the processing of personal data.
    - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller.
    - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.
    - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation.
    - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects.
    - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.
    - The controls that we, with reference to the delimitation of TimeLog A/S' services would have been designed and implemented by the data controllers, and which, if necessary to achieve the control objectives, are identified in the description.
    - The other aspects of the control environment, risk assessment process, information systems and communication, control activities and monitoring controls that are relevant to the processing of personal data.

2. Includes relevant information on changes in TimeLog A/S' services and the related technical and organisational measures and other controls throughout the period

3. Does not omit or distort information relevant to the scope of TimeLog A/S' services and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of TimeLog A/S' services that the individual data controllers might consider important in their environment.

TimeLog A/S confirms that the technical and organisational measures and other controls related to the control objectives stated in the accompanying description were suitable designed for the period 1 July 2023 to 30 June 2024. The criteria we used in making this statement were that:

1. The risks threatening achievement of the described control objectives 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 applied consistently as designed, including manual controls were performed by persons with appropriate competencies and rights, in the entire period from 1 July 2023 to 30 June 2024.

TimeLog A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, good practices for the data processing of data and relevant requirements for Data processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Copenhagen, 18 September 2024

TimeLog A/S
Per-Henrik Nielsen
Per-Henrik Ole Nielsen
CEO

3. TIMELOG A/S' DESCRIPTION OF PROCESSING ACTIVITY FOR THE SUPPLY OF TIMELOG

TIMELOG A/S

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

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

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

TIMELOG A/S AND PROCESSING OF PERSONAL DATA

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

TimeLog develops and sells own software, used by our customers for optimizing their business through structured time recording, financial project management, competent resource management, invoicing, and integration with the customer's other systems.

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

TimeLog processes personal data on behalf of its clients, who are Data processors when they apply the TimeLog platform for the software solution. TimeLog has entered into data processing agreements with the Controllers on this processing.

The personal data being processed fall within article 6 of the General Data Protection Regulation on ordinary personal data and include personal name, e-mail, telephone number, expenses, travel information, registration of work hours and normal absence. Users of the system can also choose to register health details.

MANAGEMENT OF THE SECURITY OF PERSONAL DATA

TimeLog has prepared requirements for establishing, implementing, maintaining and improving a management system for the security of personal data, which ensure compliance with the concluded agreements with the Controllers, good data processor practice, and relevant requirements for Data processors in accordance with the General Data Protection Regulation and the Danish Data Protection Act.

The technical and organisational security measures and other controls for protection of personal data are designed in accordance with the risk assessments and implemented to ensure confidentiality, integrity, and accessibility together with compliance with current data protection legislation. Security measures and controls are wherever possible automated and technically supported by IT systems.

Management of the security of personal data and the technical and organisation security measures and other controls are structured in the following key areas, for which control objectives and control activities have been defined:

THE DATA PROCESSING AGREEMENT	CONTROL AREA	ARTICLE
Control area A Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the incoming data processor agreement.	• Entering into a data processing agreement with the Controller • Instruction for processing of personal data • Compliance with instruction for processing of personal data • Communication of unlawful instruction to the controller	• Art. 28 (3) • Art. 28 (3)(a) • Art. 29 • Art. 32 (4) • Art. 28 (10) • Art. 28 (3)(h)
Control area B Procedures and controls are followed, which ensure that the data processor has implemented technical measures to ensure relevant processing security.	• Risk Assessment • Contingency plans in case of physical or technical incidents • Physical access control • Logical access control • Remote workplaces and remote access to systems and data • External communication connections • Encryption of personal data • Firewall • Network security • Anti-virus program • Vulnerability scanning and penetration testing • Back-up and re-establishment of data • Maintenance of system software • Logging in systems, databases, and network, including logging of application of personal data • Monitoring • Repair and service as well as disposal of IT equipment • Testing, assessment and evaluation of the efficiency of the technical and organisational security measures • Information security in development and changes • Segregation of development, test and production environments • Personal data in development and test environments • Support assignments	• Art. 28 (3)(c) • Art. 25
Control area C Procedures and controls are followed, which ensure that the data processor has implemented organisational measures to ensure relevant processing security.	• Information Security Policy • Review of the information security policy • Organisation of information security policy • Recruitment of employees • Resignation of employees • Training and instruction of employees processing personal data • Awareness and information campaigns for employees • Confidentiality and secrecy agreement with employees • Obligations of security of processing and impact assessments. • Audit and inspection • Records of processing activities • Storage of the record • The Danish Data Protection Agency's access to the record • Selection of Data protection officer • The position of the Data protection officer. • Tasks of the Data protection officer	• Art. 28(1) • Art. 28 (3)(b) • Art. 28 (3)(f) • Art. 28 (3)(h) • Art. 30 (2), (3) and (4) • Art. 33 (2) and (5) • Art. 38 • Art. 39
Control area D	• Deletion of personal information	• Art. 28 (3)(g)

THE DATA PROCESSING AGREEMENT	CONTROL AREA	ARTICLE
Procedures and controls are followed, which ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.	• Return of personal information	
Control area E Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.	• Storage of personal data • Handling of input and output data materials	• Art. 28 (3)(c)
Control objectives F Procedures and controls are followed, which ensure that only approved sub-data processors are used, and that the data processor, by following up on their technical and organizational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.	• Sub data processor agreement and instruction • Approval of sub data processors • Changes to approved sub data processors • Overview of approved sub data processors • Supervision of sub data processors	• Art. 28 (2) and (4)
Control area G Procedures and controls are followed to ensure that the data processor only transfers personal data to third countries or international organizations in accordance with the agreement with the data controller on the basis of a valid transfer basis.	• The data subjects' rights • Instructions from the data controller • Valid transfer basis	• Art. 44 - 49
Control area H Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion or restriction of information on the processing of personal data to the data subject.	• The data subject's rights	• Art. 28 (3)(e)
Control area I Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the data processor agreement entered into.	• Notification of personal data breaches • Assistance to the data controller in relation to personal data breaches	• Art. 33 (2) • Art. 28 (3)(f)

RISK ASSESSMENT

TimeLog has prepared a risk assessment to document the company's risk-based approach to the choice of security measures for the protection of physical persons in connection with the processing of personal data and the free movement of such data. The purpose of the risk assessment is therefore to ensure that TimeLog's procedures and implemented security measures comply with the risks that TimeLog's processing of personal data causes the data subjects. By assessment of TimeLog's relevant risk and threat-categories, existing and already implemented security measures have been considered, and we therefore refer to further statement on this.

It is Management's responsibility to take initiatives to address the threat scenario that TimeLog is facing at all times, so that the security measures and controls introduced are appropriate, and the risk personal data breach, is reduced to a proper level.

The appropriate level of security is assessed on a current basis. The assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.

An annual risk assessment is performed as the basis of updating of the technical and organisational security measures and other controls. The risk assessment illustrates the probability and consequences of incidents that may threaten the security of personal data and thereby natural persons' rights and freedoms, including incidental, intentional, and unintentional events. The risk assessment considers the actual technical level and implementation costs.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

The technical and organisational security measures and other controls concern all processes and systems, which process personal data on behalf of the Controller. The control objectives and control activities stated in the control schedule are an integral part of the subsequent description.

The Data processor's guarantees

TimeLog has introduced policies and procedures ensuring that TimeLog can provide the sufficient guarantees for completing appropriate technical and organisational security measures in such a way that the processing complies with the requirements of the General Data Protection Regulation and ensures protection of the data subject's rights. TimeLog has established an organisation of the security of personal data as well as prepared and implemented an information security policy approved by Management, which is reviewed and updated on an ongoing basis. Procedures for recruiting and resignation of employees as well as guidelines for training and instruction of employees processing personal data, including completion of awareness and information campaigns, exist.

Data processing agreement

TimeLog has introduced policies and procedures for entering into data processing agreements, which ensure that TimeLog in relation to the client contract enters into a data processing agreement, which states the terms for processing of personal data on behalf of the Controller. TimeLog applies a template for data processing agreements in accordance with the services to be provided, including information on the use of subprocessors. The data processing agreements are digitally signed and stored electronically.

Instruction for processing of personal data

TimeLog has introduced policies and procedures ensuring that TimeLog acts according to the instruction given by the Controller in the data processing agreement. The instruction is maintained with procedures instructing employees in how processing of personal data must be done, including who at the Controller may give binding instructions to TimeLog. Moreover, the procedures ensures that TimeLog informs the Controller, when their instructions are not perceived to be following data protection legislation.

Sub-processors

TimeLog has introduced policies and procedures which ensure that sub-processors are assigned the same data protection obligations as stated in the data processor agreement between the Controller and TimeLog and that the sub-processor may give sufficient guarantees to protection of personal data. Procedures ensure that the Controller gives a preceding specific or general written approval of sub processors, including changes of approved sub processors are controlled.

TimeLog assesses the sub-processor and their guarantees, before an agreement is entered into, to ensure that the sub-processor will be able to comply with the obligations assigned TimeLog. TimeLog monitors their sub-processor on an annual basis based on a risk assessment of the specific processing of personal data by obtaining auditor reports of the type ISAE 3000 or SOC 2, or similar documentation.

Confidentiality and professional secrecy

TimeLog has introduced policies and procedures ensuring confidentiality at the processing of personal data. All employees at TimeLog have committed to confidentiality by signing an employment contract containing terms of secrecy and confidentiality.

Technical and organisational security measures

Risk Assessment

TimeLog has completed the technical and organisational security measures on the basis of an assessment of risk in connection to confidentiality, integrity and availability. Please refer to separate section about this.

Contingency plans

TimeLog has established contingency plans, thus, TimeLog can re-establish the availability of and access to personal data in due time in case of physical and technical events. TimeLog has established emergency preparedness, which takes effect in these cases. Organisation of an emergency preparedness group is established and guidelines for activation of the emergency preparedness has been introduced.

TimeLog has designed detailed contingency plans and plans for re-establishment of systems and data, which among other things ensure person independence in connection with activation of the emergency preparedness and the re-establishment. A copy of the plans is stored securely outside TimeLog's IT systems. The plans are tested and revised on a current basis in connection with changes to systems, etc.

Storage of personal data

TimeLog has introduced procedures ensuring that personal data are solely stored in accordance with the contract with the Controller and the list of locations in the accompanying data processing agreement.

Physical access control

TimeLog has introduced procedures ensuring that rooms are protected against unauthorised access. Only persons with a work-related or other legitimate need have access to the rooms, and special security measures have been taken for areas, where personal data is processed. Clients, suppliers, and other visitors must be escorted.

Physical security

TimeLog has introduced procedures to ensure that servers are protected from unauthorized access, damage, outages, and similar incidents by special security measures. Thus, servers are stored in a specially designed server room with physical and electronic access control and logging of accesses. The server room is protected against environmental threats such as fire, water intrusion, moisture, overheating, power failure and over-voltage. Systems for environmental protection of operating facilities are serviced and maintained on an ongoing basis in accordance with the regulations of the respective suppliers. The operating environment is monitored.

Logical access security

TimeLog has introduced procedures ensuring that access to systems and data are protected by an authorisation system. User is set up with unique user identification and password, and user identification is used in connection with allocation of resources and systems. All allocation of rights in systems is based on a work-related need. An assessment of the users' continued work-related need for access is reviewed at least once annually, including relevancy and correctness of allocated user rights. Procedures and controls support the process of creating, changing, and terminating users and allocated rights as well as review hereof.

The design of rules for i.a. length, complexity, regular changes to and history of password and termination of user account after unsuccessful log-on attempts follows best practice for a secure logical access control. Technical measures have been established to support these rules.

Remote workplaces and remote access to systems and data

TimeLog has procedures ensuring that access from workplaces outside TimeLog's premises and remote access to systems and data take places through VPN connections.

External communication connections
TimeLog has introduced procedures to ensure that external communications connections are secured with strong encryption and that email and other communications containing sensitive personal information are encrypted in the transmission using TLS.

Encryption of personal data
TimeLog Name has introduced procedures ensuring that databases containing personal data are encrypted and that the same apply for back-up copies. Recovery keys and certificates are securely stored.

TimeLog has introduced procedures ensuring that data on personal units, which are not protected by special security measures, is encrypted when put into use, so that access to data is only possible for authorised users. Recovery keys and certificates are stored properly.

Algorithms and levels of encryption used for encryption of units, servers, and data are risk assessed on a current basis according to the current threat level.

Firewall
TimeLog has introduced procedures ensuring that traffic between the internet and the network is controlled by a firewall. External access by means of ports in the firewall is limited wherever possible, and access rights are allocated through actual ports for specific segments. Workstations uses firewall.

Network security
TimeLog has introduced procedures ensuring that networks in relation to use and security are divided into several virtual networks (VLAN), in which traffic between the individual virtual networks are controlled by firewalls. Servers with incorporated firewalls use this to ensure that access is only given to necessary services.

Anti-virus program
TimeLog has introduced procedures ensuring that units with access to networks and applications are protected against virus and malware. Antivirus programmes and other protective systems are continually updated and adjusted in relation to the actual threat level, and an ongoing monitoring of these systems has been set up, including periodical testing for functionality.

Vulnerability scanning
TimeLog has introduced procedures ensuring that a periodic portscanning for the purpose of identifying and prevent technical vulnerabilities in the infrastructure, thus, losses of confidentiality, integrity, and accessibility of systems and data are avoided.

Back-up and re-establishment of data
TimeLog has introduced procedures ensuring that systems and data are backed up to prevent loss of data or loss of accessibility in the event of critical failures. Back-ups are stored at an alternative location. Back-ups are protected with both physical and logical security measures, which prevent data from falling into the hands of unauthorised persons or that back-ups are destroyed by fire, water, malicious damage, or accidental damage.

Maintenance of system software
TimeLog has introduced procedures ensuring that system software is updated regularly according to the suppliers' directions and recommendations. Procedures for Patch Management include operating systems, critical services and software installed on servers and workstations.

Logging in systems, databases, and network
TimeLog has introduced procedures ensuring that logging is set up in accordance with legislative requirements and business needs, based on a risk assessment of systems and the actual security alert status. The scope and quality of log data are sufficient to identify and demonstrate possible unauthorised use of systems or data, and log data is examined on a current basis for applicability and abnormal conduct. Log data is secured against loss and erasure.

Monitoring
TimeLog have introduced procedures ensuring that continuing monitoring of systems and technical security measures introduced.

Testing, assessment and evaluation
TimeLog has introduced procedures for regular testing, assessment and evaluation of the efficiency of the technical and organisational security measures for ensuring the processing security.

Data protection by design and by default

TimeLog has introduced policies and procedures for developing and maintaining the TimeLog platform, which ensure a controlled change of process. A change management system for controlling development and change tasks is applied, and every task follows a uniform process initiated by a risk assessment in accordance with the requirements of data protection by design and by default.

Development, testing, and production environments are separate, and segregation of duties is established between employees in the development department and the operation and support department. Each development and change task pass through a testing cycle and anonymised production data are applied as test data. Procedures are introduced for version control, logging and back-up, thus, it is possible to reinstall previous versions.

Deletion and return of personal data

TimeLog has introduced policies and procedures ensuring that personal data are deleted or returned in accordance with instruction from the Controller, when the processing of personal data terminates at the end of contract with the Controller.

Assistance to the Controller

TimeLog has introduced policies and procedures ensuring that TimeLog can assist the Controller in complying with their obligation to reply to requests on executing the data subjects' rights.

TimeLog has introduced policies and procedures ensuring that TimeLog can assist the Controller in ensuring compliance with the obligations of article 32 on security of processing, article 33 on notification and communication of personal data breach, and article 34 - 36 on data protection impact assessment.

TimeLog has introduced policies and procedures ensuring that TimeLog can provide to the Controller all information necessary to demonstrate compliance with the requirements of the Data processors. Besides, TimeLog allows and assists in audits, including inspections performed by the Controller or others, who are authorised to do this by the Controller.

Records of processing activities

TimeLog has introduced policies and procedures ensuring that a record is kept of categories of processing activities performed on behalf of the Controller. The record is updated regularly and controlled during the annual review of policies and procedures, etc. The record is stored electronically and can be provided for the supervisory authority, by request.

Communication of personal data breach

TimeLog has introduced policies and procedures ensuring that personal data breaches are registered with detailed information about the event and that the Controller communicates without undue delay after Company Name becomes aware of the personal data breach. The registered information makes the Controller able to assess whether the personal data breach must be reported to the supervisory authority and whether the data subjects should be notified.

Data Protection Officer

TimeLog does not employ a Data Protection Officer (DPO) since the company's core business does not include personal data processing and due to the requirements for having a DPO are not valid for TimeLog's business.

Transfer of personal data to third countries

TimeLog has put in place policies and procedures to ensure that the transfer of personal data to sub-processors in non-EU countries takes place in accordance with EU-US Privacy, standard contract or other valid transfer basis and as instructed by the controller.

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

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

COMPLEMENTARY CONTROLS WITH THE CONTROLLER

The Controller 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:

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

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has inspected procedures to obtain evidence of the information in TimeLog A/S' description of TimeLog A/S' services, the design and operating effectiveness of the relating technical and organisational measures and other controls. The procedures selected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed or operating effectively.

BDO's test of the design and the operating effectiveness of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related the control objectives and related control activities selected by TimeLog A/S, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that related controls were appropriately designed and operated effectively for the period 1 July 2023 to 30 June 2024.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation and effectiveness hereof were performed by inquiries, inspection, observation and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel 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.

With respect to the services provided by Amazon Web Service within e-mail service, we have from independent auditor received the SOC 2 for the sub-processor's technical and organisational security measures and other controls for the period from 1 April 2023 to 31 March 2024.

With respect to the services provided GlobalConnect A/S within hosting service, we have from independent auditor received the ISAE 3000 for the sub-processor's technical and organisational security measures and other controls for the period from 1 January 2023 to 31 December 2023.

With respect to the services provided by Microsoft within operating systems, we have from independent auditor received the SOC 2 for the sub-processor's technical and organisational security measures and other controls for the period from 1 October 2022 to 31 September 2023.

With respect to the services provided by HubSpot within Customer service software, we have from independent auditor received the SOC 2 for the sub-processor's technical and organisational security measures and other controls for the period from 1 May 2023 to 30 April 2024.

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

With respect to the services provided by Unit IT A/S within outsourcing services division, we have from independent auditor received the SOC 2 for the sub-processor's technical and organisational security measures and other controls for the period 1 January 2023 to 31 December 2023.

These sub-processor's relevant control objectives and related controls are not included in TimeLog A/S' description of TimeLog A/S' services and relevant controls related to operation of TimeLog A/S' services. Thus, we have solely assessed the reports and tested the controls at TimeLog A/S, which ensures appropriate supervision of the sub-processor's compliance with the data processing agreement made between the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the following exceptions noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective, and
- 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.

Control area A

Control Objective

- *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered into.*

Control activities	Test performed by BDO	Result of test
Entering into a data processing agreement with the Controller ▶ The Data processor has procedures for entering into written data processing agreements which are in accordance with the services provided by the Data processor. ▶ The Data processor applies a data processing agreement template for entering into data processor agreements. ▶ When entering a written data processing agreement based on the data controllers' template, the data processor uses a checklist to ensure that it can comply with the data processing agreement. ▶ Data processing agreements are stored electronically. ▶ Data processing agreements contain information about the use of sub processors.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for entering into a data processing agreements and observed that the data processor handles personal data on behalf of the data controller in accordance with the provisions of the data processing agreement. We have inspected the data processor's template for data processing agreements and observed that the data processor uses the Danish Data protection agency's template for data processing agreements. We have inspected the data processor's template for data processing agreements and observed that the data processor uses the Danish Data Protection Agency's template for data processing agreements as a checklist to ensure compliance with the requirements By random sampling we have inspected data processing agreements and observed that they are stored electronically. By random sampling we have inspected data processing agreements and observed that they contain information about the use of sub-processors.	No exceptions noted.
Instruction for processing of personal data ▶ Data processing agreement contains instructions from data controller(s). ▶ The Data processor obtains instruction for processing personal data from the Controller, in connection with entering into a data processor agreement.	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

Control area A

Control Objective

- *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered into.*

Control activities	Test performed by BDO	Result of test
	We have inspected the data processor's template for a data processing agreement and observed that it contains instructions regarding the processing of personal data. By random sampling, we have inspected data processing agreements and observed that the data processor obtains instructions for the processing of personal data.	
Compliance with instruction for processing of personal data - The Data processor solely processes personal data as per instruction from the Controller. - The Data processor has created and implemented written procedures regarding processing personal data to ensure that data is only processed based on instructions from data controllers. - The Data processor procedures are looked over and updated regularly and at least annually. - The Data processor verifies that it complies instructions in active data processing agreements.	We have made inquiries of relevant personnel at the data processor. By random sampling, we have inspected the data processing agreements and observed that the data processor performs the processing of personal data according to the data controller's instructions. We have inspected the data processor's procedure for data processing agreements and observed that the data processor processes personal data according to the instructions from the data controller. We have inspected the data processor's annual cycle of controls and observed that the data processor's procedure for data processing agreements is reviewed and updated annually. We have inspected the data processor's internal procedures for when the organisation acts as a data processor and observed that these procedures are designed to ensure and demonstrate compliance with the data processing agreements and relevant laws.	No exceptions noted.

Control area A		
Control Objective ▶ *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered into.*		
Control activities	**Test performed by BDO**	**Result of test**
Communication of unlawful instruction to the Controller ▶ The Data processor has prepared a procedure for communication to the Controller when the Controller's instruction is in contravention of the data protection legislation. ▶ The Data processor communicates immediately to the Controller, if the Controller's instruction is in contravention of the data protection legislation.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for data processing agreements and observed that the data processor must immediately notify the data controller if the instructions conflict with data protection regulations. Upon inquiry, we have been informed that there have been no instances of unlawful instructions during the declaration period. Therefore, we have not been able to implementation and effectiveness.	We have noted that the data processor has established a procedure for unlawful instructions. We have not been able to test the implementation and effectiveness of the control, as there have been no instances of unlawful instructions during the declaration period. No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Risk Assessment ▶ On an ongoing basis, risk assessment of potential risks for the accessibility, confidentiality and integrity of data is performed, in relation to the data subjects' rights and freedoms. ▶ The vulnerability of systems and processes is assessed based on identified threats. ▶ Risks are minimised based on the assessment of their likelihood and consequence. ▶ Risk assessments are updated on an ongoing basis when needed, but at least once a year.	We have made inquiries of relevant personnel at the data processor. We have inspected the risk assessments prepared by the data processor and observed that these risk assessments include risks to data accessibility, confidentiality, and integrity concerning the rights and freedoms of data subjects. We have inspected the risk assessment and observed that evaluations of potential threats have been prepared, where these threats are identified based on their consequence and likelihood. We have inspected that the risk assessment has been reviewed during the declaration period and observed this review is part of the data processor's annual cycle of control.	No exceptions noted.
Contingency plans in case of physical or technical incidents ▶ The Data processor has established a contingency plan, which ensures quick response time to restore the accessibility of and access to personal data in a timely manner, in case of a physical or technical incident. ▶ The Data processor has established periodic testing of the contingency plan with a view to ensure that the contingency plans are up-to-date and efficient in critical situations. ▶ Tests of the contingency plans are documented and evaluated.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has established a contingency plan and observed that the data processor has set recovery times for systems. We have inspected the data processor's contingency plan and observed that the data processor has defined the responsibilities for roles that should be contacted in case of an incident. We have inspected the data processor's annual cycle of control and observed that the contingency plan is reviewed annually. We have inspected that the data processor holds Disaster Recovery Meetings in relation with testing the contingency plan.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected that the data processor has performed test of the contingency plan and observed that this test is documented and evaluated.	
Physical access control ▶ There is established physical access control, which reduced the possibility for unauthorised access to the Data processor's offices, facilities and personal data. Only authorised personnel has access. ▶ A regular and amnual control of the physical access security measures is performed.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for physical access control an observed the data processor 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. We have inspected that GlobalConnect, in addition to providing hosting services for the data processor, obtains an annual ISAE 3402 and ISAE 3000 reports. We have inspected the auditor reports ISAE 3402 and ISAE 3000 for GlobalConnect and observed that there are no remarks regarding the physical access controls.	No exceptions noted.
Logical access control ▶ The Data processor has implemented procedures for user administration which ensures that user creation and deletion follows a uniformed process and that all user creations are authorised. ▶ User rights are assigned based on work-related needs. ▶ Privileged user rights are assigned based on work-related needs. ▶ Users and user rights are reviewed regularly. ▶ All access to systems and data is logged.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for user administration and observed that the data processor follows a uniformed process and alle user creations are authorised. By random sampling, we have inspected user creation and observed that the data processor allocates the access rights to users according to work related needs.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
▶ The data processor has established logical access control for systems with personal information, including two-factor authentication. ▶ The data processor has established rules for password requirements, which must be followed by all employees.	We have inspected the data processor'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 data processor and observed that the data processor has a limited number of users with privileged rights, and these users have a work-related need for such access. We have inspected the procedure for review of user access rights and observed that the review should be performed regularly. We have inspected that the data processor has performed review of user access rights during the declaration period. We have inspected that event logs recording user activities, exceptions, faults, and information security events are generated, retained, and monitored. We have inspected the data processor's policy for secure log-on and observed that multi-factor-authentication is required to access the data processor's systems. We have inspected the established requirements for passwords and observed that these requirements are enforced for all employees and external consultants.	
Remote workplaces and remote access to systems and data ▶ All mobile units which have access to personal data must have anti-virus installed and updated. ▶ Remote access to the Data processor's systems and data is via an encrypted VPN connection. ▶ Remote access must go through two-factor authentication.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's information security policy and observed that the data processor continuously monitors that antivirus software is installed and updated.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected the data processor's devices and observed that antivirus software is installed on them. We have inspected the data processor's teleworking policy and observed that a VPN must be used for remote access to the data processor's production environment. We have inspected that it is not possible to access the data processor's production environment without using a VPN.	
External communication connections ▶ External access to systems and databases, which are used to process personal data, is done through firewall and VPN. ▶ External communication connections are encrypted. ▶ The Data processor has an overview of which external communication connections are approved to access their network.	We have made inquiries of relevant personnel at the data processor. We have inspected that external access to systems and databases used to process personal data is protected with a firewall and VPN. We have inspected that the external communication connections are encrypted. We have inspected the data processor's network topology and observed that employees must use a VPN to access the production environment, ensuring that only approved external communication connections can access their network.	No exceptions noted.
Encryption of personal data ▶ The Data processor has implemented an encryption policy for encryption of personal data. The policy defines the strength and protocol for encryption. ▶ Portable media with personal data are encrypted. ▶ When transmitting confidential and sensitive personal data via the internet and e-mail, encryption is applied.	We have made inquiries of relevant personnel at the data processor. We have inspected the policy for cryptographic controls and observed that the data processor has encrypted web connections between server and services using HTTPS.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected that the data processor uses encryption on removable media for the storage of personal data. We have inspected the data processor'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.	
Firewall ▶ The Data processor has configured firewall according to best practise. ▶ The Data processor only use services/ports which are needed. ▶ Firewalls are configured and validated periodically when needed, thus, service/ports only are open when needed.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's firewall configuration and observed, that the firewall is according to best practice. We have inspected the data processors routers and access points and observed that the only use services/ports which are needed.	We have found that there is no documentation regarding that the firewall has been configured and validated during the declaration period. No further exceptions noted.
Network security ▶ 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 Data processor's network is segmented so that internal services/servers cannot communicate directly with the internet. ▶ The Data processor uses known network technologies and mechanisms to protect internal network.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's network topology and observed that the servers that run applications cannot be accessed directly from the Internet. We have inspected the data processor's network and observed that the network has been segmented into a guest network and an administrative network, which cannot directly communicate with each other directly. We have inspected the data processor's network topology and observed that the data processor uses mechanisms such as firewalls and VPNs to protect the internal network.	No exceptions noted.

Control area B

Control Objective

- *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*

Control activities	Test performed by BDO	Result of test
Anti-virus program ▶ Anti-virus software is installed on all servers and workstations. ▶ Anti-virus software is updated on an ongoing basis and updated with the latest version.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's information security policy and observed that the data processor continuously monitors that antivirus software is installed and updated. We have inspected the data processor's devices and observed that antivirus software is installed on them.	No exceptions noted.
Vulnerability scanning and penetration testing ▶ At least once a year vulnerability scanning/port scanning of the Data processor's network is performed. The result is documented in a report. ▶ The Data processor reviews the report and follows up on ascertained weaknesses. ▶ The Data processor processes/handles/mitigates any vulnerabilities based on a risk assessment. ▶ The Data processor has documented their handling/mitigation of weaknesses found.	We have interviewed relevant personnel with the Data processor. We have inspected the data processor's procedure for vulnerability scanning and observed that vulnerability scans are conducted at quarterly by an external party, with the results documented in a report. By random sampling, we have inspected that the data processor reviews the vulnerability scanning reports and follows up on identified weaknesses, mitigating any vulnerabilities based on a risk assessment. We have inspected that the data processor has documented their handling and mitigation of weaknesses found.	No exceptions noted.
Back-up and re-establishment of data ▶ Back-up of systems and data is performed daily. ▶ Operation and storage of back-ups are outsourced to sub data processor.	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected the data processor'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 data processor regularly tests backups. We have inspected that the data processor has performed restore tests during the declaration period. We have inspected the data processor's backup policy and observed that storage of backups is outsourced to sub-processor.	
Maintenance of system software ▶ The Data processor keeps and overview of operating system software/ third party programmes on workstations and servers which is updated continuously. ▶ Operating system software on servers and workstations is constantly updated. ▶ The data processor has implemented a system software update process to ensure system availability and security.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor keeps an up-to-date list of operating software and third-party programs on workstations and servers. We have inspected that the data processor'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 data processor's operational systems on a weekly basis.	No exceptions noted.
Logging in systems, databases, and network, including logging of application of personal data ▶ All successful and failed attempts to access the Data processor's systems and data are logged. ▶ All user changes in systems and databases are logged.	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
▶ The log is deleted after the determined retention period. ▶ The Data processor monitors and logs network traffic.	We have inspected that event logs recording user activities, exceptions, faults, and information security events are generated, retained, monitored, and deleted according to the retention period. We have inspected that the data processor monitors and logs network traffic.	
Monitoring ▶ The Data processor has established a monitor system for monitoring of production environments, including uptime, performance, and capacity. ▶ The Data processor is notified of identified alerts and follows up on these.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's capacity management procedure and observed that the data processor monitors the collected metrics. By random sampling, we have inspected a selection of alerts collected by the data processor from monitoring and observed that the data processor has ensured the system performance is maintained.	No exceptions noted.
Repair and service as well as disposal of IT equipment ▶ The data processor disposes of IT equipment by physical destruction of data-bearing media. ▶ The data processor securely deletes data on data-bearing media (overwriting / distortion, encryption...) ▶ The data processor maintains a list of destroyed IT equipment.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedures for disposal and repair 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 data processor 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.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Testing, assessment and evaluation of the efficiency of the technical and organisational security measures ▶ The Data processor tests, assesses and evaluates the efficiency of whether the technical and organisational security measures are appropriate in relation to the data handled on behalf of the Controller.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for testing, assessing, and evaluating the effectiveness of security measures and observed that the procedure aims to ensure that the security measures are appropriate and effective for the data processed on behalf of the data controller. We have inspected that the data processor annually prepares a summary of the ISAE 3000 GDPR report, where the data processor reviews and evaluates the results of the tests conducted in the ISAE 3000 report.	No exceptions noted.
Development and sustainability of systems ▶ The Data processor works on the basis of privacy-by-design principles in development and maintenance tasks. ▶ Risk assessment of system changes has been performed to ensure data protection through design and default settings.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's policy for a secure development environment, where developers can request customer data, but if these developers are outside the EU, the customer data must be anonymised. We have inspected the data processor's procedure for development and observed that development and change tasks must be verified before being deployed to the production environment.	No exceptions noted

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Information security in development and changes ▶ A rollback plan is implemented in case of errors in the production environment. ▶ The Data processor minimises attack surfaces by relating to functionalities and open service usability in development and modification tasks. ▶ User creation takes place as a starting point with the lowest user rights level. ▶ Only the Data processor's developers have access to source code.	We have made inquiries of relevant personnel at the data processor. We have inspected that a rollback plan is implemented in case of error in the data processor's productions environment. We have inspected the data processor's development process and observed that development and change tasks must be verified before being deployed to the production environment. By random sampling, we have inspected development and change tasks and observed that these were verified before being deployed to the production environment. By random sampling, we have inspected user creations and observed that the data processor creates users with the lowest user right as a starting point. We have inspected that only relevant employees have access to the source code.	No exceptions noted.
Segregation of development, test and production environments ▶ Segregation of duties between development and operation has been introduced. ▶ Changes to functionality are tested before being put in operation. ▶ Development and test are performed in development environments, which are segregated from production systems. ▶ A version management system is used to register all changes in source code.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor'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.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected the data processor's network topology and observed that the data processor has segmented their development environment, test environment, and production environment. We have inspected the data processor's use of a version control system and observed that all changes to the source code are registers.	
Personal data in development and test environments ▶ Fictional test data or anonymised data are used in development and test environments.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for using test data and observed that personal data and customer data must be anonymized in the test environment. We have inspected that the data processor's uses anonymized test data.	No exceptions noted.
Support assignments ▶ Supporters access and handling of personal data is given based on support tickets and the supports work related need.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's support flow and observed the data processor has listed ticket types. By random sampling, we have inspected support tickets and observed that the data processor accesses personal data based on a work-related need.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Information Security Policy ▶ The Data processor has prepared and implemented an information security policy.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has implemented an information security policy and observed that its purpose is to support the data processor'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.
Review of the information security policy ▶ The Data processor's information security policy is reviewed and updated at least once annually.	We have made inquiries of relevant personnel at the data processor. We have inspected that the information security policy is reviewed within the declaration period. We have inspected the data processor's annual cycle of control and observed that the information security policy is reviewed annually.	No exceptions noted.
Organisation of information security policy ▶ The Data processor has documented and established management control of information security.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's contingency plan and observed that the data processor has delegated the responsibilities and roles for information security to individual employees.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected that the data processor's Chief Executive Officer has reviewed the information security policy and observed that the Chief Executive Officer has signed and approved the information security policy.	
Recruitment of employees ▶ The Data processor performs screening of potential employees before employment. ▶ The Data processor performs background check in accordance with the Data processors procedure and the function, which the candidate is to take.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's policy for screening and recruiting employees and observed that the data processor is required to perform screening of potential candidates through interviews and skill assessments. By random sampling we have inspected that the data processor has performed screening of new employees with interviews and tested them with a skills assessment.	No exceptions noted.
Resignation of employees ▶ The Data processor has prepared and implemented a procedure for resignation of employees the end of the employment. ▶ At resignation, the employee is informed that the signed confidentiality agreement is still applicable.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's employee offboarding procedure and observed that the data processor 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 data processor 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.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Training and instruction of employees processing personal data ▶ The Data processor conducts awareness training of new employees in accordance with data protection and information security, in continuation of the employment. ▶ The Data processor conduct's introduction courses for new employees, regarding how data controllers are to process data. ▶ The Data processor conducts training of employees on an ongoing basis in accordance with data protection and information security and handling hereof.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor uses training modules and observed that these modules include topics related to information security. We have inspected that the data processor has introductory modules for awareness available and observed that all employees have completed this module.	No exceptions noted.
Awareness and information campaigns for employees ▶ The Data processor conducts awareness training in the form of morning meetings, notices, etc. ▶ The Data processor performs information campaigns for employees on data protection and information security.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for awareness training and observed that the data processor continuously conducts training for employees regarding information security. We have inspected that the data processor performs information campaigns for employees regarding data protection and information security.	No exceptions noted.
Legal duty of confidentiality ▶ All employees are subjected statutory duty of confidentiality under the provisions of the Danish Criminal Code.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's template for employee contracts and observed that employees are required to adhere to the statutory duty of confidentiality under the provisions of the Danish Criminal Code.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Confidentiality and secrecy agreement with employees ▶ All employees have signed an employment contract, which contains a section regarding confidentiality ▶ External suppliers/consultants are subject to professional secrecy when entering into cooperation.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's template for employee contracts and observed that employees agree to confidentiality regarding the data processor's business. By random sampling we have inspected the employment contracts and observed that they 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 data processor for the execution of their consulting purposes.	No exceptions noted.
Audit and inspection ▶ The Data processor is obligated to prepare an ISAE 3000 assurance report on the technical and organisational security measures aimed at processing and protection of personal data. ▶ The Data processor assists the Controller at physical supervision by making available resources. ▶ The Data processor makes available the information necessary to the Controller and the supervisory authorities upon request, in connection with audit and inspection of the Data processor.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor prepares an ISAE 3000 assurance report on the technical and organisational security measures. We have inspected the data processor's template for data processing agreement and observed that the data processor assists the data controller with physical supervision by making resources available.	We have noted that the data processor has responsibility to assist the data controller and the Danish Data protection Agency. We have not been able to test the implementation and effectiveness of the control, as there have been no request from the data controller and the Danish Data Protection Agency during the declaration period. No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	Upon inquiry, we have been informed that the data processor has not received requests regarding physical inspection. Thus, we have not been able to test implementation and effectiveness. We have inspected data processor's template for data processing agreement and observed that data processor makes information available to the data controller and the Danish Data protection Agency. Upon inquiry, we have been informed that data processor has not received the request from the Danish Data Protection Agency. Thus, we have not been able to test implementation and effectiveness.	
Records of processing activities ▶ The Data processor has established a record of processing activities as Data processor. ▶ The record is updated with significant changes continuously. ▶ The record is updated at least once a year during the annual review.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has established a record over categories of processing activities as a data processor. We have inspected that the record has been updated in the declaration period. We have inspected the data processor's annual cycle of controls and observed that the record is updated at least once a year.	No exceptions noted.
Storage of the record ▶ The record is stored electronically on the Data processor's system/file drive.	We have made inquiries of relevant personnel at the data processor. We have inspected that the record of processing activities is stored electronically.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
The Danish Data Protection Agency's access to the record ▶ The Data processor hands over the record at the request of the Danish Data Protection Agency.	We have made inquiries of relevant personnel at the data processor. We have inspected data processor's template for data processing agreement and observed that data processor to the hands over the record at the request of the Danish Data Protection Agency on request. Upon inquiry, we have been informed that data processor has not received the request from the Danish Data Protection Agency. Therefore, we have not been able to test implementation and effectiveness.	We have noted that the data processor has responsibility to assist the Danish Data protection Agency with access to the record. We have not been able to test the implementation and effectiveness of the control, as there have been no request from the Danish Data Protection Agency during the declaration period. No exceptions noted.

Control area D		
Control Objective ▶ *To ensure that the Data processor can delete and return personal data when the service regarding the processing has terminated, in accordance with instruction from the Controller.*		
Control activities	**Test performed by BDO**	**Result of test**
Deletion of personal data ▶ The Data processor deletes the Controller's personal data per instruction, at termination of the main agreement.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's template for data processing agreements and observed that, upon termination of agreement, the data processor is obligated to delete the data controller's personal data. By random sampling, we have inspected terminated agreements and observed, that the data processor deletes the controller's personal data after the termination of agreement.	No exceptions noted.
Return of personal data ▶ The Data processor returns the Controller's personal data as per instruction, at termination of the main agreement. ▶ The data controller and data processor have agreed in which format, transfer and media data is to be returned when requested by the data controller.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's policy for deletion and return of personal data and observed that personal data must either be deleted or returned. Upon inquiry, we have been informed that the data processor has not received any request from data controller regarding return of personal data. Thus, we have not been able to test implementation.	We have noted that the data processor has established a policy for deletion and return of personal data. We have not been able test the implementation and effectiveness of the control, as there have been no return of personal data during the declaration period. No exceptions noted.

Control area E

Control Objective

- *Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.*

Control activities	Test performed by BDO	Result of test
Storage of personal data ▶ Personal data is contained so it is unavailable for unauthorised personnel. ▶ The Data processor's personal data can only be accessed based on one's work-related need. ▶ Confidential digital personal data is kept in encrypted format. ▶ Personal data is kept only as long as there is a legitimate reason for the use/storage.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has assigned user access to personal data based on the employee's work-related need. We have inspected that the data processors have encrypted the data storage on mobile devices. We have inspected that the data processor's productions environment is protected with encryption. We have inspected that the data processor keeps personal data as long as there is a legitimate reason for the use or storage.	No exceptions noted.
Handling of input and output data materials ▶ The Data processor ensures that input data and output data is handled with confidentiality. ▶ The Data processor ensures that input data and output data is handled by authorised persons. ▶ The Data processor ensures that the integrity of the input data and output data is verified. ▶ Input data and output data are ensured confidentiality through encryption.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's information security policy and observed that all personal data must be treated with confidentiality. We have inspected that a part of the hiring process requires new employees to acknowledge that they have read the service data processor's information security policy. By random sampling we have inspected that new employees during the declaration period have acknowledged that they have read the data processor's information security policy.	No exceptions noted.

Control area E		
Control Objective ▶ *Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected that the data processor has assigned user access for handling input and output data and observed that only authorized persons receive these rights. We have inspected that the data processor ensures the confidentiality and integrity of input and output data through encryption.	

Control area F		
Control Objective ▶ *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Sub-processor agreement and instruction ▶ When using sub processors, the Data processor enters into a sub data processing agreement, which assigns the same data protection obligations to the sub processor as the Processor is assigned. ▶ Instructions from the Controller is disclosed to the sub processor. ▶ The data processing agreement with the sub processor is stored electronically. ▶ The data processing agreement with the sub processor contains information about the use of sub processors.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has entered sub-processing agreements with the sub-processors and observed, that the sub-processors are subject to the same data protection obligations as the data processor, and that the instructions have been passed on to the sub-processors. We have inspected that the sub data processing agreement is stored electronically. We have inspected entered sub data processing agreements and observed these contains information regarding the use of sub processors.	No exceptions noted.
Approval of sub-processors ▶ The Data processor only use approved sub processors.	We have made inquiries of relevant personnel at the data processor. By random sampling we have inspected data processing agreements and observed that the data processor only uses approved sub-processors.	No exceptions noted.
Changes to approved sub-processors ▶ The Data processor has prepared an appropriate process with the Controller for change of approved sub processors. ▶ The Data processor communicates to the Controller when changing sub processors in connection with general approval of sub processor.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's procedure for changing sub-processors and observed that the data processor communicates these changes to the data controllers.	No exceptions noted.

Control area F

Control Objective

- *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*

Control activities	Test performed by BDO	Result of test
▶ The Controller may object to changing sub processor. ▶ When changing sub processor, the Data processor must have this approval from the Controller.	We have inspected that the data processor is required to notify the data controller of any changes to sub-processors, allowing the data controller the opportunity to object. We have inspected the data processor's communication with data controllers regarding changes in approved sub-processors and observed that the data processor has informed data controllers about changes to sub-processors in the data processing agreement.	
Overview of approved sub-processors ▶ The Data processor has an overview of approved sub processors. Overview of approved sub processors contains among other things information about location for processing and type of processing, which the sub processor undertakes.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has an overview of approved sub-processors in the template for data processing agreements and observed that it includes the location and type of processing of personal data.	No exceptions noted.
Supervision of sub-processors ▶ The Data processor exercises supervision, including obtains and reviews the sub processor's audit opinions, certifications, etc. ▶ The Data processor exercises supervision of the sub processor at least once annually.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor’s procedure for supervision of sub-processors and observed, that the data processor must conduct regular supervision of sub-processors to ensure ongoing compliance with the General Data Protection Regulation (GDPR) and the terms of data processing agreement. We have inspected that the data processor has conducted supervision of sub-processors and observed that the data processor has obtained audit reports from sub-processors.	We have found that the data processor has not conducted supervision of HubSpot. No further exceptions noted.

Control area F

Control Objective

- *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*

Control activities	Test performed by BDO	Result of test
	We have inspected documentation for supervision of sub-processors and observed that the data processor has addressed the results from the audit reports. We have inspected the Amazon Web Services SOC 2 report for the period 1 April 2023 to 31 March 2024. We have inspected the Microsoft SOC 2 report for the period 1 October 2022 to 30 September 2023. We have inspected GlobalConnect's ISAE 3000 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 3000 for the period 1 January 2023 to 31 December 2023.	

Control area G		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor only transfers personal data to third countries or international organisations in accordance with the agreement with the data controller on the basis of a valid transfer basis.*		
Control activities	**Test performed by BDO**	**Result of test**
Procedures for transfer to transfer of data to third countries or international organisations ▶ Written procedures exist for the transfer of personal data to third countries or international organisations in accordance with the agreement with the data controller on the basis of a valid transfer basis. ▶ The Data processor's procedure is reviewed and assessed on an ongoing basis, and at least once a year, whether the procedure needs to be updated.	We have made inquiries of relevant personnel at the data processor. We have inspected data processor's template for data processing agreement and observed that the data processor only carries out third-country transfers according to the data controller's instructions. We have inspected that the template for data processing agreement is updated continuously and at least annually.	No exceptions noted.
Instructions from the data controller ▶ The Data processor only transfers personal data to third countries or international organisations on the instructions of the data controller. ▶ The Data processor documents instructions obtained regarding the transfer of personal data to third countries or international organisations from data controllers.	We have made inquiries of relevant personnel at the data processor. We have inspected data processor's template for data processing agreement and observed that third country transfers can only take place on the instructions of the data controller. We have inspected entered data processing agreements and observed that third country transfer can take place on the on the basis of the EU-U.S. Data Privacy Framework.	No exceptions noted.
Valid transfer basis ▶ The Data processor assesses and documents that a valid transfer basis exists in connection with the transfer of personal data to third countries or international organisations.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's list of sub-processors and observed that the data processor uses four sub-processors where third country transfers can take place. These sub-processors are Amazon Web Service, Microsoft, HubSpot, Pendo and Inscale.	We have found that Amazon Web Services, Microsoft and HubSpot have adopted the new transfer basis, the EU-U.S. Data Privacy Framework, which came into effect on July 10, 2023. The data processor has stated that before July 10, 2023, no transfers of personal data to non-secure third countries took place, and that they have configured and implemented security measures to

Control area G		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor only transfers personal data to third countries or international organisations in accordance with the agreement with the data controller on the basis of a valid transfer basis.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected that Amazon Web Services, Microsoft and HubSpot are certified under the EU-U.S. Data Privacy Framework, providing the data processor a valid basis for transferring the data controller's personal data to the sub-processors Amazon Web Services, Microsoft and HubSpot. We have observed that Pendo is not certified under EU-U.S. Data Privacy Framework, and therefore, the data processor does not have a valid basis for transferring the data controller's personal data to the sub-processor Pendo. We have inspected that the data processor's transfer impact assessments regarding Inscale and Pendo and observed that no supplementary measures have been implemented.	protect personal data when using Amazon Web Services Microsoft and HubSpot as sub-processors. We have found that the data processor uses Pendo as sub-processor without a valid transfer basis in cases where data controllers give instructions to allow third country transfers. No further exceptions noted.

Control area H

Control Objective

- *Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion, or restrictions of information on the processing of personal data to the data subject.*

Control activities	Test performed by BDO	Result of test
The data subjects' rights ▶ The Data processor has prepared a procedure for assistance to the Controller at fulfilling the data subjects' rights. ▶ It is possible to provide insight into all information registered in (system/service).	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has prepared a procedure to assist data controllers in fulfilling the rights of data subjects. Upon inquiry, we have been informed that the data processor has not received any request from data controller regarding fulfilling the data subject's rights. Therefore, we have not been able to test implementation and effectiveness.	We have noted that the data processor has established a procedure to assist data controllers in fulfilling the rights of data subjects. We have not been able to test the implementation and effectiveness of the control, as there have been no request from data controller regarding fulfilling the data subject's rights during the declaration period. No exceptions noted.

Control area I

Control Objective

- *Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the relevant data processor agreement.*

Control activities	Test performed by BDO	Result of test
Communication of personal data breach ▶ The Data processor communicates to the Controller the personal data breach without undue delay. ▶ The Data processor updates the Controller on all information relevant and necessary when the information is available to the Data processor. ▶ Communication between Data processor and Controller is documented and stored.	We have made inquiries of relevant personnel at the data processor. We have inspected data processor's template for data processing agreement and observed that the data processor communicates the personal data breach to the data controller without undue delay. We have inspected the data processor's procedure for handling personal data breaches and observed that the breach handling process must be documented, and the data processor must be able to provide this documentation upon request. Upon inquiry we have been informed that no personal data breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and efficiency.	We have noted that the data processor has established a procedure for handling personal data breaches. We have not been able to test the implementation and effectiveness of the control, as there have been no personal data breaches during the declaration period. No exceptions noted.
Identification of personal data breaches ▶ The Data processor has prepared a procedure for assessing and identifying personal data breaches.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has prepared a procedure for assessing and identifying personal data breaches. Upon inquiry we have been informed that no personal data breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and efficiency.	We have noted that the data processor has established a procedure for assessing and identifying personal data breaches. We have not been able to test the implementation and effectiveness of the control, as there have been no personal data breaches during the declaration period. No exceptions noted.

Control area I		
Control Objective ▶ *Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the relevant data processor agreement.*		
Control activities	**Test performed by BDO**	**Result of test**
Registration of personal data breaches ▶ The Data processor registers personal data breaches in the data breach log. ▶ The Data processor has prepared and implemented a procedure for experience gathering when personal data is breached.	We have made inquiries of relevant personnel at the data processor. We have inspected that the data processor has implemented a log for registering personal data breaches. We have inspected the data processor's data breach log procedure and observed that key components are established in the data processor's breach log, such as Response Actions, Investigation Results, and Follow-up Actions, which are used to gather experience from recorded breaches. Upon inquiry we have been informed that no personal data breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and efficiency	We have noted that the data processor has established a data breach log procedure. We have not been able to test the implementation and effectiveness of the control, as there have been no personal data breaches during the declaration period. No exceptions noted.
Assisting the data controller with handling personal data breaches ▶ Procedures for assistance to the Controller when assisting in relation to articles 33-34 and 36 have been prepared.	We have made inquiries of relevant personnel at the data processor. We have inspected data processor's template for data processing agreement and observed that the data processor assist the data controller in relation to articles 33-34 and 36. Upon inquiry we have been informed that no personal data breaches have occurred during the declaration period. Therefore, we have not been able to test implementation and efficiency	We have noted that the data processor has established a processor assisting the data controller in relation to articles 33-34 and 36. We have not been able to test the implementation and effectiveness of the control, as there have been no personal data breaches during the declaration period. 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 3000 declaration, TimeLog has the following supplementary information:

Control activity	Result of test	Comment of the company
Firewall ▶ The Data processor has configured firewall according to best practise. ▶ The Data processor only use services/ports which are needed. ▶ Firewall are configured and validated periodically when needed, thus, service/ports only are open when needed.	We have found that there is no documentation regarding that the firewall has been configured and validated during the declaration period.	We acknowledge the auditor's finding regarding the lack of documentation for the configuration and validation of the firewall during the declaration period. While we confirm that the firewall was indeed configured and validated as per our internal procedures and best practices, we recognise that we did not maintain adequate documentation to substantiate this activity during the relevant period. Moving forward, we will ensure that all configuration and validation processes are appropriately documented and maintained to provide evidence of compliance with the control activities.
Supervision of sub-processors ▶ The Data processor exercises supervision, including obtains and reviews the sub processor's audit opinions, certifications, etc. ▶ The Data processor exercises supervision of the sub processor at least once annually.	We have found that the data processor has not conducted supervision 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-processors, 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.
Valid transfer basis ▶ The Data processor assesses and documents that a valid transfer basis exists in connection with the transfer of personal data to third countries or international organisations.	We have found that Amazon Web Services, Microsoft and HubSpot have adopted the new transfer basis, the EU-U.S. Data Privacy Framework, which came into effect on July 10, 2023. The data processor has stated that before July 10, 2023, no transfers of personal data to non-secure third countries took place, and that they have configured and implemented security measures to protect personal data when using Amazon Web Services Microsoft and HubSpot as sub-processors. We have found that the data processor uses Pendo as sub-processor without a valid transfer basis in cases where data controllers give instructions to allow third country transfers.	We acknowledge the auditor's finding regarding the transfer basis for Pendo. While we confirm that we have conducted a Transfer Impact Assessment (TIA) for Pendo, we recognize that a valid transfer mechanism is not currently in place for transfers to third countries. We are in close dialogue with Pendo regarding this matter, and they are actively working towards joining the EU-U.S. Data Privacy Framework. In the meantime, we continue to assess and mitigate risks by implementing additional security measures where necessary to protect personal data. We are committed to ensuring that all transfers are compliant with applicable regulations as Pendo finalizes its alignment with the privacy framework

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk