Visma DataLøn A/S

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreements with Visma DataLøn's clients, from 01.01.2021 to 30.09.2021

Contents

1 Management's statement

Visma DataLøn processes personal data for Visma DataLøn's clients in accordance with the data processing agreement (A1a DPA 1.feb-2021.pdf and Vilkår DataLøn_1. august2021.pdf)

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

Visma DataLøn uses subservice organizations for data storage (Atea), infrastructure (VITC), and internal IT services and physical security regarding local office facilities (Visma Consulting). The Description includes only the control objectives and related controls of Visma DataLøn and excludes the control objectives and related controls of the subservice organization. Certain control objectives specified in the Description can be achieved only if subservice organization controls assumed in the design of our controls are suitably designed and operating effectively. The Description does not extend to controls of the subservice organization.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Visma DataLøn's controls are suitably designed and operating effectively, along with related controls at the data processor. The Description does not extend to controls of the data controller.

Visma DataLøn confirms that:

a) The accompanying description in section 3, fairly presents the Dataløn system, which has processed personal data for data controllers subject to the Regulation throughout the period from 01-01-2021 to 30-09-2021. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the DataLøn system was designed and implemented, including:

   - The types of services provided, including the type of personal data processed;
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
   - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects;
   - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
   - Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
   - Controls that we, in reference to the scope of Visma DataLøn, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;

- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data;

(ii) Includes relevant information about changes in the Data Processor's the DataLøn system in the processing of personal data in the period from 01-01-2021 to 30-09-2021;

(iii) Does not omit or distort information relevant to the scope of the Dataløn system being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the Dataløn system that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 01-01-2021 to 30-09-2021, if controls at subservice organisations are working effectively, and data controller applied the complementary user entity controls assumed in the design of Visma DataLøn's controls throughout the period from 01-01-2021 to 30-09-2021. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 01-01-2021 to 30-09-2021.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Copenhagen, 26. januar 2022

Karina Wellendorph

Managing Director

2 Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with Visma DataLøn's clients.

To: Visma DataLøn and Visma DataLøn's clients

Scope

We were engaged to provide assurance about Visma DataLøn's description in section 3 of the Dataløn system in accordance with the data processing agreement with Visma DataLøn's clients throughout the period from 01-01-2021 to 30-09-2021 ("the Description") and about the design and operating effectiveness of controls related to the control objectives stated in the Description. We express reasonable assurance in our conclusion.

The Description indicates that certain control objectives can only be achieved if the complementary user entity controls assumed in the design of Visma DataLøn's controls are suitably designed and operating effectively, along with related controls at Visma DataLøn. Our engagement did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Visma DataLøn uses subservice organizations for data storage (Atea), infrastructure (VITC) and internal IT services and physical security regarding local office facilities (Visma Consulting). The Description includes only the Control Objectives and related controls of Visma DataLøn and excludes the control objectives and related controls of subservice organizations. Certain Control Objectives specified by Visma DataLøn can be achieved only if subservice organization controls assumed in the design of Visma DataLøn's controls are suitably designed and operating effectively, along with the related controls at Visma DataLøn. Our engagement did not extend to controls of subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such subservice organization controls.

Visma DataLøn's responsibilities

Visma DataLøn is responsible for: preparing the Description and the accompanying statement in section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria presented in the statement, and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

We apply the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Our responsibilities

Our responsibility is to express an opinion on Visma DataLøn's Description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of the system Visma DataLøn and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively.

Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in section 1.

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

Limitations of controls at a data controller

Visma DataLøn'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 Visma DataLøn system that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

(a) The Description fairly presents the DataLøn system as designed and implemented throughout the period from 01-01-2021 to 30-09-2021;

(b) The controls related to the control objectives stated in the Description were suitably designed throughout the period from 01-01-2021 to 30-09-2021 to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 01-01-2021 to 30-09-2021, if relevant controls at subservice organisations are working effectively, and customers applied the complementary user entity controls assumed in the design of Visma DataLøn's controls throughout the period 01-01-2021 to 30-09-2021; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 01-01-2021 to 30-09-2021, if relevant controls at subservice organisations are working effectively, and complementary user entity controls at the data controller assumed in the design of Visma DataLøn's controls operated effectively throughout the period 01-01-2021 to 30-09-2021.

Description of tests of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for data controllers who have used Visma DataLøn, who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Copenhagen, 26. januar 2022
EY
Godkendt Revisionspartnerselskab
CVR no.: 30 70 02 28

Jesper Due Sørensen
Partner, CISA

Nils B. Christiansen
statsaut. revisor
mne34106

3 Description of processing

Visma DataLøn A/S supplies DataLøn, a standard IT system that runs payroll for more than 60,000 customers, including more than 500,000 payslips per month.

The system consists of a payroll system that performs calculations, submits reports to authorities and generates payslips. The DataLøn system includes:

- Standard set-up to cover the customer's payroll needs
- Possibility of unlimited sample calculations
- Updates to ensure compliance with Danish legislation
- Possibility of payroll processing with mandatory and optional reporting to third parties, including authorities and pension companies
- Return of data in electronic format
- Support on system use and for payroll processing.

Visma DataLøn A/S uses external suppliers, including ATEA A/S and Visma IT & Communications (VITC) for certain parts of the IT delivery (data storage and infrastructure). These suppliers are managed through Visma Enterprise Operations' department, which includes IT infrastructure, as well as external suppliers.

In May 2021 Visma DataLøn A/S moved into Visma House in Carlsbergbyen, Copenhagen, with other Visma Companies. From then Visma Consulting has been the supplier of internal IT services and physical security measures, following the same joint Visma Group policy as before the move.

Visma DataLøn A/S uses an internal system ("CRM") for customer management. CRM provides an overview of customers, subscription status, support cases created and similar information. The system is used by Visma DataLøn A/S' customer service and marketing.

For access control, SSO is used, which is our common single sign-on module, which uses DataLøn frontends and APIs.

The system contains user information as well as rights (claims).

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is the delivery of a standard IT solution which, on the basis of the customer's reports to Visma DataLøn, performs payroll processing for the customer, in accordance with Visma DataLøn's terms and conditions (Main Agreement).

The nature of the processing

The Data Processor's processing of personal data on behalf of the Data Controller concerns payroll processing, and includes:

- calculation of employee pay;
- make all calculations and reports, and facilitate money transfers to SKAT, ATP, holiday and maternity funds, pension funds, etc. on the customer's behalf;
- report statistics to the employers' association and Statistics Denmark on behalf of customer;
- send payslips to the Employees' e-Boks;
- store the customer's payslips in an electronic archive for five years after the end of the year in which the payslip is produced;
- provide assistance for the start-up and creation of the customer and the employees;
- provide support and consulting services via telephone and online from Visma DataLøn's payroll consultants whenever the customer needs help.

Visma DataLøn does not develop or adapt DataLøn in relation to the customer's specific needs or wishes.

Personal data

- General personal data
    - identification data
    - master data (employment data)
    - holiday pay settlement
    - pension settlement
    - tax settlement
    - account information
- Other personal data
    - CPR numbers

Categories of data subjects covered by the Data Processor agreement:

- Customer employees
- Customer contact person

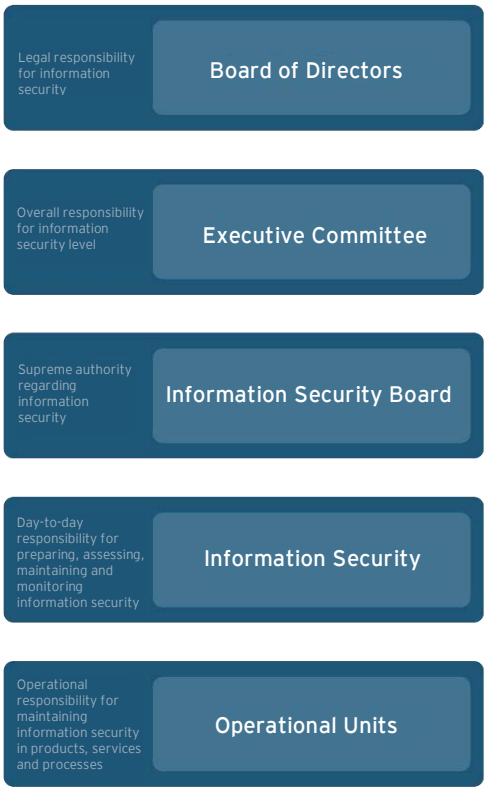
Practical measures

Visma DataLøn has established a management framework for initiating and managing implementation as well as operation of information security and data protection.

Responsibility for data protection and information security is handled by Visma DataLøn's Information Security Board, as well as the Data Protection Manager and the Security Manager. The area is also supported by the Visma Group DPO.

Visma DataLøn has implemented policies, controls and processes that cover the following information security areas:

- Organisation of information security
- Personnel safety
- Asset management
- Access control
- Cryptography
- Physical security and environmental protection
- Operational reliability
- Communication security
- Procurement, development and maintenance of systems
- Supplier relations
- Management of information security breaches
- Information security aspects of emergency preparedness and re-establishment management
- Compliance



Risk assessment

The purpose of Risk Assessment is to provide direction, expectations and intentions for managing information security risks in Visma DataLøn.

- Assessed security risks must be analysed.
- Threats and vulnerabilities must be assessed.
- Consequences (positive or negative) of risk for targets.
- Consequences (positive or negative) of risk for assets.
- The probability that these consequences may occur.

In those specific cases where a high risk involves the Data Controller having to carry out an impact assessment regarding data protection, it is also described how the Data Processor may have assisted with this.

Reporting and follow-up on security risks must be performed in accordance with the defined needs of the Division and Group.

Control measures

Visma DataLøn A/S has based their controls on the FSR ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement, and included several controls regarding technical security measures based on ISO27001.

The method for performing risk management in Visma DataLøn is based on internationally recognised principles and standards that are adapted to the organisation. The method provides guidance and includes processes on how effective risk management should be performed.

- Control objective A
  There are procedures and controls that ensure that instructions regarding the processing of personal data can be complied with in accordance with the Data Processor agreement in force.
- Control objective B
  There are procedures and controls that ensure that Visma DataLøn has implemented technical measures to ensure relevant processing security.
- Control objective C
  There are procedures and controls that ensure that Visma DataLøn has implemented organisational measures to ensure relevant processing security.
- Control objective D
  There are procedures and controls that ensure that personal data can be deleted or returned if an agreement is reached with the Data Controller.
- Control objective E
  There are procedures and controls that ensure that Visma DataLøn only store personal data in accordance with the agreement with the Data Controller.
- Control objective F
  Procedures and controls are followed which 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 objective G
  Procedures and controls are followed, which ensure that the Data Processor can assist the Data Controller with the disclosure, correction, deletion or restriction of information about the processing of personal data of the registered person.
- Control objective H
  Procedures and controls are followed which ensure that any security breaches can be handled in accordance with the Data Processor agreement in force.

Complementary controls at the Data Controllers

The Data Controller is responsible for ensuring that the processing of Personal Data meets the requirements of the General Data Protection Regulation and the Data Protection Act.
The Data Controller is, by using the services provided by Visma DataLøn in accordance with the Main Agreement, obliged to process Personal Data in accordance with the provisions of applicable legislation, including, e.g., by:

- ensuring that the processing of Personal Data complies with the Data Protection Regulation;
- ensuring that the data subjects are informed about the processing of Personal Data;
- ensuring that the instruction is lawful in relation to the personal data legislation in force at any given time;
- ensuring that the instruction is appropriate in relation to this Data Processor agreement and the main service;
- ensuring that the Data Controller's users are up to date;
- ensuring that they have established detailed procedures for safeguarding the rights of the data subject

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

Our work was performed in accordance with ISAE 3000, Assurance Engagements other than audits or reviews of historical financial information.

Our test of the controls' design and implementation comprised the control objective and related controls, which have been selected by Management and which are stated below. Any other control objectives, related controls and controls at Visma DataLøn is not covered by our tests.

The tests performed in connection with the determination of design and operating effectiveness of controls are outlined below.

4.2 Tests performed

Below, we have summarised the tests performed by EY in order to assess controls relevant to Visma DataLøns information security and measures pursuant to the data processing agreement.:

Inspection	Reading of documents and reports which contain disclosure on the performance of the control. This work includes i.a. the reading of and position-taking to reports and other documentation to assess whether specific controls have been designed in a way that allow them to be effective, if implemented. Furthermore, we assess whether controls are adequately monitored at suitable intervals. As to the technical platforms, databases and network components, we tested the specific system set-up to ensure that controls were implemented and operating effectively throughout the audit period. Our tests comprised i.a. an assessment of the patching level, services allowed, segmenting, password complexity, etc. In addition, we inspected equipment and premises physically.
Inquiries	Inquiries of suitable staff with Visma DataLøn. Inquiries comprised i.a. the performance of controls.
Observation	We observed the performance of controls.

4.3 Control objectives, control activity, tests and test results

Control objective A Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.			
No.	*Visma DataLøn's control activity*	*Test performed by EY*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. Inspected that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing. Inspected that procedures are up to date.	No deviations noted.
A.2	Visma DataLøn only processes personal data stated in the instructions from the data controller.	Inspected that Management ensures that personal data are only processed according to instructions.	No deviations noted.

Control objective A Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.			
No.	*Visma DataLøn's control activity*	*Test performed by EY*	*Result of test*
A.3	Visma DataLøn immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	Inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. Inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. Inquired if there have been any cases where the processing of personal data was evaluated to be against legislation.	We have been informed that there have been no cases within the audit period, where the instructions from the data controllers infringes the Regulation or other European Union or member state data protection provisions. No deviations noted.
A.4	Relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Inspected that relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements are explicitly identified, documented and kept up to date for each information system and the organization. Inspected a sample of quarterly meetings, where relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements are discussed.	No deviations noted.
A.5	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Inspected that privacy and protection of personally identifiable information is ensured as required in relevant legislation and regulation where applicable. Inspected minutes of meetings for a sample of quarterly status group meetings, where it was discussed whether legislation and regulations are relevant and applicable for Visma Dataløn's clients.	No deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures exist to ensure establishment of the safeguards agreed. Inspected that procedures are up to date. Inspected that the safeguards agreed have been established.	No deviations noted.
B.2	Visma DataLøn has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	Inspected that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Inspected that the risk assessment performed is up to date and comprises the current processing of personal data. Inspected a sample of identified risks to ensure that they were managed appropriately. Inspected that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. Inspected that the data processor has implemented the safeguards agreed with the data controller.	No deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed. Inspected that antivirus software is up to date. Inspected test results on anti-malware controls in latest audit reports from service providers Atea (responsible for antivirus on production environments) and VITC (responsible for antivirus on local PC's).	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. Inspected that the firewall has been configured in accordance with the relevant internal policy. Inspected test results on firewall controls in latest audit reports from service providers Atea (responsible for firewall around production environments) and VITC (responsible for firewall on local network).	No deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.5	Access to personal data is isolated to users with a work-related need for such access.	Inspected that formalised procedures are in place for restricting users' access to personal data. Inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. Inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Inspected a sample of users' access to systems and databases that such access is restricted to the employees' work-related need.	No deviations noted.
B.6	For the systems and databases used for the processing of personal data, system monitoring, log documentation overview and dashboard including summary of logging activities are established.	Inspected that, for systems and databases used in the processing of personal data, system monitoring has been established. Inspected test results on controls related to logging in latest audit reports from service providers Atea (responsible for logging on production environments) and VITC (responsible for logging on infrastructure). Inspected that a log documentation overview and dashboarding including summary of logging activities is established.	Log monitoring and dashboard was not implemented during the audit period. No further deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.7	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. Inspected that technological encryption solutions have been available and active throughout the audit period. Inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the audit period and whether the data controllers have been appropriately informed thereof.	No deviations noted.
B.8	Logging of the following matters has been established in systems, databases and networks: ► Activities performed by system administrators and others holding special rights; ► Security incidents comprising: - Changes in log setups, including disabling of logging; - Changes in users' system rights; - Failed attempts to log on to systems, databases or networks; - Transactions made by all types of users - including unusual behavior ► Application behavior Logon data are protected against manipulation and technical errors and are reviewed regularly.	Inspected that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs. Inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. Inspected that user activity data collected in logs are protected against manipulation or deletion. Inspected that logging have been configured throughout the audit period. Inspected test results on controls related to logging in latest audit reports from service providers Atea (responsible for logging on production environments) and VITC (responsible for logging on infrastructure).	A periodic review of activities performed by system administrators has not been performed within the audit period. No further deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.9	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Inspected a development or test databases that personal data included therein are pseudonymised or anonymised. Inquired if there are any development or test databases in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.	No deviations noted.
B.10	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	Inspected that formalised procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Inspected for a sample of changes that the established change management procedures were followed. Inspected extracts from technical security parameters and setups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches. Inspected test results on controls related to patching in latest audit reports from service providers Atea (responsible for security patching on production environments) and VITC (responsible for security patching on infrastructure).	No deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.11	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	Inspected that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data. Inspected a sample of employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists. Inspected a sample of resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis. Inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No deviations noted.
B.12	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	Inspected that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Inspected documentation that, throughout the audit period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed. Inspected test results on controls related to physical security in latest audit report from service provider Atea (responsible for physical security on production environments).	No deviations noted.
B.13	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Inspected that a classification scheme is maintained and has been made available for employees. Inspected that the classification scheme has been reviewed and approved.	No deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.14	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Inspected that a register is maintained that lists: ▶ confidentiality level ▶ how access is managed ▶ who can grant access. Inspected that the register has been reviewed and approved.	No deviations noted.
B.15	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Inspected that an asset register is maintained that includes relevant information and information processing assets. Inspected that the asset register is reviewed annually.	No deviations noted.
B.16	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Inspected that all types of identified assets are listed in the acceptable use policy. Inspected that updates to the acceptable use policy is communicated to employees.	No deviations noted.
B.17	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Inspected that a formal and documented Business Continuity Plan is maintained reviewed and approved annually. Inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No deviations noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
B.18	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Inspected that a formal and documented Business Continuity Plan is maintained, reviewed and approved annually. Inspected that a Business Impact Assessment has been performed to establish the requirements of the Business Continuity Plan.	No deviations noted.
B.19	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Inspected that underlying procedures for the business continuity are reviewed and updated. Inspected that the underlying procedures have been tested to ensure that they are valid and effective during adverse situations.	No deviations noted.

Control objective C Procedures and controls are complied with to ensure that Visma DataLøn has implemented organisational measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.1	Management of Visma DataLøn has approved a written information security policy that has been communicated to all relevant stakeholders, including Visma DataLøn's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	Inspected that an information security policy exists that Management has considered and approved within the past year. Inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C.2	Management of Visma DataLøn has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. Inspected a sample of data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.

Control objective C Procedures and controls are complied with to ensure that Visma DataLøn has implemented organisational measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.3	The employees of Visma DataLøn are screened as part of the employment process. Such screening comprises, as relevant: ► References from former employers; ► Certificates of criminal record; ► Diplomas	Inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. Inspected a sample of data processing agreements that the requirements therein for screening employees are covered by the data processor's screening procedures. Inspected a sample of new employees appointed during the audit period that documentation exists of the screening having comprised: ► References from former employers; ► Certificates of criminal record; ► Diplomas;	No deviations noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	Inspected for a sample of employees appointed during the audit period that the relevant employees have signed a confidentiality agreement. Inspected for a sample of employees appointed during the audit period that the relevant employees have been introduced to: ► Information security policy; ► Procedures for processing data and other relevant information.	No deviations noted.

Control objective C Procedures and controls are complied with to ensure that Visma DataLøn has implemented organisational measures to safeguard relevant security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.5	For resignations or dismissals, Visma DataLøn has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. Inspected for a sample of employees resigned or dismissed during the audit period that rights have been deactivated or terminated and that assets have been returned.	No deviations noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by Visma DataLøn for the data controllers.	Inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Inspected for a sample of employees resigned or dismissed during the audit period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	2 out of a sample of 5 resigned employees, did not receive a written notification upon their resignation that their confidentiality agreement remains valid. No further deviations noted.
C.7	Awareness training is provided to Visma DataLøn's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No deviations noted.

Control objective D Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Inspected that the procedures are up to date.	No deviations noted.
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: ► Deletion of recordings of phone conversations after 6 months ► Deletion of primary input data after 45 days	Inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. Inspected a sample of data processing sessions from the data processor's list of processing activities that documentation exists that personal data are stored in accordance with the agreed storage periods. Inspected a sample of data processing sessions from the data processor's list of processing activities that documentation exists that personal data are deleted in accordance with the agreed deletion routines.	No deviations noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: ► Returned to the data controller; and/or ► Deleted if this is not in conflict with other legislation.	Inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. Inspected for a sample of terminated data processing sessions during the audit period that documentation exists that the agreed deletion or return of data has taken place.	No deviations noted.

Control objective E Procedures and controls are complied with to ensure that Visma DataLøn will only store personal data in accordance with the agreement with the data controller.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. Inspected that the procedures are up to date. Inspected a sample of data processing sessions from the data processor's list of processing activities that documentation exists that data processing takes place in accordance with the data processing agreement.	No deviations noted.
E.2	Data processing and storage by Visma DataLøn must only take place in the localities, countries or regions approved by the data controller.	Inspected that the data processor has a complete and updated list of processing activities stating localities, countries or regions. Inspected a sample of data processing sessions from the data processor's list of processing activities that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No deviations noted.

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, Visma DataLøn ensures adequate security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.1	Written procedures exist which include requirements for Visma DataLøn when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Observed that procedures are up to date.	No deviations noted.
F.2	Visma DataLøn only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	Inspected that the data processor has a complete and updated list of sub-data processors used. Inspected a sample of sub-data processors from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No deviations noted.
F.3	When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from Visma DataLøn. When changing the specially approved sub-data processors used, this has been approved by the data controller.	Inspected that formalised procedures are in place for informing the data controller when changing the sub-data processors used. Inspected documentation that the data controller was informed when changing the sub-data processors used throughout the audit period.	No deviations noted.

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, Visma DataLøn ensures adequate security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.4	Visma DataLøn has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Inspected existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list. Inspected a sample of sub-data processing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.
F.5	Visma DataLøn has a list of approved sub-data processors disclosing: ▶ Name; ▶ Business Registration No.; ▶ Address; ▶ Description of the processing.	Inspected that the data processor has a complete and updated list of sub-data processors used and approved. Inspected that, as a minimum, the list includes the required details about each sub-data processor.	No deviations noted.

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, Visma DataLøn ensures adequate security of processing.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, Visma DataLøn regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	Inspected that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. Inspected documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. Inspected documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on. Inspected documentation that information on the follow-up at sub-data processors is communicated to the data controller so that such controller may plan an inspection.	No deviations noted.

Control objective G Procedures and controls are complied with to ensure that Visma DataLøn can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
G.1	Written procedures exist which include a requirement that Visma DataLøn must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. Inspected that procedures are up to date.	No deviations noted.
G.2	Visma DataLøn has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	Inspected that the procedures in place for assisting the data controller include detailed procedures for: ▶ Handing out data; ▶ Correcting data; ▶ Deleting data; ▶ Restricting the processing of personal data; ▶ Providing information about the processing of personal data to data subjects. Inspected that requests by the data controller for assistance in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects have been documented in a correct and timely manner.	No deviations noted.

Control objective H Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
H.1	Written procedures exist which include a requirement that Visma DataLøn must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Inspected that procedures are up to date. Inspected relevant sub-service providers' data processing agreements.	No deviations noted.
H.2	Visma DataLøn has established the following controls to identify any personal data breaches: ► Awareness of employees; ► Monitoring of network traffic; ► Follow-up on logging of access to personal data; ► Monitoring of Dark Web and relevant fora	Inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. Inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. Inspected documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on on a timely basis. Observed that dark web and relevant online fora are scanned for potential personal data leaks.	Log monitoring and dashboard was not implemented during the audit period. No further deviations noted.

Control objective H Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
H.3	If any personal data breach occurred, Visma DataLøn informed the data controller without undue delay and no later than 24 hours after having become aware of such personal data breach at Visma DataLøn or a sub-data processor.	Inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. Inquired whether sub-data processors have identified any personal data breaches throughout the audit period. Inspected that the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents. Inspected that a sample of personal data breaches recorded at the data processor or the sub-data processors have been communicated to the data controllers concerned without undue delay and no later than 24 hours after the data processor became aware of the personal data breach.	No deviations noted.

Control objective H Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
H.4	Visma DataLøn has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: ► Nature of the personal data breach; ► Probable consequences of the personal data breach; ► Measures taken or proposed to be taken to respond to the personal data breach.	Inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: ► Describing the nature of the personal data breach; ► Describing the probable consequences of the personal data breach; ► Describing measures taken or proposed to be taken to respond to the personal data breach. Inspected documentation that, when a personal data breach occurred, measures were taken to respond to such breach.	No deviations noted.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Karina Wellendorph
Managing Director
På vegne af: Visma DataLøn A/S
Serienummer: PID:9208-2002-2-480460597825
IP: 176.22.xxx.xxx
2022-01-26 09:48:13 UTC
NEM ID

Nils Bonde Christiansen
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: PID:9208-2002-2-243192639174
IP: 145.62.xxx.xxx
2022-01-26 09:59:19 UTC
NEM ID

Jesper Due Sørensen
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: PID:9208-2002-2-421950499915
IP: 80.62.xxx.xxx
2022-01-26 10:00:56 UTC
NEM ID