www.pwc.dk

Visma Acubiz A/S

Independent auditor's ISAE 3000 assurance report on information security and measures as at 31 December 2023 pursuant to the data processing agreement with data controllers

March 2024

acubiz

Contents

1. Management's statement

Visma Acubiz A/S processes personal data on behalf of data controller in accordance with the data processing agreements.

The accompanying description has been prepared for data controller who has used Acubiz Solution standard operating platform and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules") have been complied with.

Visma Acubiz A/S uses Visma IT and Progressive A/S as a subservice supplier of infrastructure operation (IaaS). This report uses the carve-out method and does not comprise control objectives and related controls that Visma IT and Progressive A/S performs for Visma Acubiz A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at customers are suitably designed with our controls. This report does not comprise the suitability of the design effectiveness of these complementary controls.

Visma Acubiz A/S confirms that:

a) The accompanying description in section 3 fairly presents Acubiz Solution standard operating platform that has processed personal data for data controllers subject to the data protection rules as at 31 December 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Acubiz Solution standard operating platform 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 security measures in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- Controls that we, in reference to the scope of Acubiz Solution standard operating platform, 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) Does not omit or distort information relevant to the scope of Acubiz Solution standard operating platform 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 Acubiz Solution standard operating platform 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 as at 31 December 2023. The criteria used in making this statement were that:

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

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

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

Copenhagen, 22 March 2024
Visma Acubiz A/S

Henrik Malling

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures as at 31 December 2023 pursuant to the data processing agreement with data controller

To: Visma Acubiz A/S and data controller

Scope

We have been engaged to provide assurance about Visma Acubiz A/S's description in section 3 of Acubiz Solution standard operating platform in accordance with the data processing agreement with data controller as at 31 December 2023 (the description) and about the design related to the control objectives stated in the description.

Our report covers whether Visma Acubiz A/S has designed appropriate controls related to the control objectives stated in section 4. The report does not include an assessment of Visma Acubiz A/S's general compliance with 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" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules").

Visma Acubiz A/S uses Visma IT and Progressive A/S as a subservice supplier of infrastructure operation (IaaS). This report uses the carve-out method and does not comprise control objectives and related controls that Visma IT and Progressive A/S performs for Visma Acubiz A/S.

Some of the control objectives stated in Visma Acubiz A/S' description in section 3 can only be achieved if the complementary controls at customers are suitably designed with Visma Acubiz A/S' controls. This report does not comprise the suitability of the design effectiveness of these complementary controls.

We have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon.

We express reasonable assurance in our conclusion.

Visma Acubiz A/S's responsibilities

Visma Acubiz A/S is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing controls to achieve the stated control objectives.

Auditor's independence and quality control

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

Our firm applies International Standard on Quality Management 1, 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 Visma Acubiz A/S's description and on the design of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000 (revised), "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed.

An assurance engagement to report on the description and the design of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its Acubiz Solution standard operating platform and about the design of controls. The procedures selected depend on the auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by the data processor and described in the Management's statement section.

As mentioned above, we have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon. 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

Visma Acubiz A/S's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Acubiz Solution standard operating platform 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.

Opinion

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

a) The description fairly presents Acubiz Solution standard operating platform as designed and implemented as at 31 December 2023; and

b) The controls related to the control objectives stated in the description were suitably designed as at 31 December 2023.

Description of test 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 Acubiz A/S's Acubiz Solution standard operating platform and 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 data protection rules have been complied with.

Aarhus, 22 March 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

3. Description of processing

The purpose of the data processor's processing of personal data on behalf of the data controller is: The data processor's processing of the data controller's personal data is done with the agreed purpose of providing the Acubiz EMS service and any related services as further described in the Main Agreement. The processing happens primarily in connection with the data controller's (including the data controller's configured Acubiz EMS users) use of the Acubiz EMS service.

Nature of processing

The data processor's processing of personal data for the data controller has the nature that follows from the Main Agreement, and among other things in particular include the following activities:

- Import and upload of the data controller's credit card transactions to Acubiz EMS (NB: Acubiz is only responsible for the transport of the transactions) as well as storage of the data in the Acubiz EMS solution.
- Making Acubiz EMS, with the data stored therein, available for the data controller's users.
- Accessing the data in connection with error correction in the Acubiz EMS solution.
- Storage of data for archiving purposes.

Personal data

The processing solely includes ordinary personal data (cf. Article 6 of the GDPR), including more specifically (depending on the data controller's specific configuration and use of the Acubiz EMS solution): name, initials, e-mail address, telephone number, address, employee number, company ID, configuration information (typically choice of language, username, password/passcode, approval limit, etc.), payment card details, bank details, and transaction data (typically information regarding amount, currency, date, country, type of cost, extract of credit card number and card holder identifier, account type, dimensions and possibly comments, as well as photo of payment document).

If the data controller has purchased the add-on service Mileage under the Main Agreement, the processing will also include ordinary personal data regarding driving, including (depending on the data controller's specific configuration and use of the Acubiz EMS solution) the purpose of the transportation, the license plate of the car (registration number), distance, the start and end address and, if location service has been chosen, GPS tracking data.

If the data controller has purchased the add-on service TIME under the Main Agreement, the processing will also include ordinary personal data regarding time registration. The composition of this data depends on the information demands specified by the data controller but can (depending on the data controller's specific configuration and use of the Acubiz EMS solution) e.g. be data on time spent with specification of account, type, dimensions and date.

The Acubiz EMS solution is only intended for processing of ordinary personal data
The data controller (including the data controller's configured users of the Acubiz EMS service) must NOT enter or cause to be entered into the Acubiz EMS solution personal data which belongs to any of the following categories, as the solution is not intended for processing of personal data of such categories:

- Sensitive personal data (personal data covered by Article 9 of the GDPR), i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
- Personal data relating to criminal convictions and offences (personal data covered by Article 10 of the GPDR)

- Data regarding CPR numbers (or regarding any other national identification numbers/identifiers of general application for which specific conditions for processing apply pursuant to Member State law, cf. Article 87 of the GDPR).

Practical and control measures

Visma Acubiz was established in 1997 and was based in Birkerød. In December 2021 Acubiz was bought by Visma and became a legal entity in Visma. Visma Acubiz moved to Visma's HQ in Copenhagen in September 2022. Visma Acubiz provides the cloud-based travel expense solution ACUBIZ SOLUTION which is an Expense Management Service.

Acubiz Solution (Standard version 7) is a web-based travel expense service, streamlining the procedures for handling travelling expenses and other employee expenses. It is provided as a hosted solution and is available to users, super users and administrators via a web interface (Internet Explorer Version 11 or newer version).

Acubiz Solution basically consists of an automatic workflow, where e-transactions and cash expenses are automatically placed with the employee, who with a few clicks may create a travel expense report, enter costs and send the travel expense report for approval and export. Thereafter, the file is ready for import into the company's financial management systems.

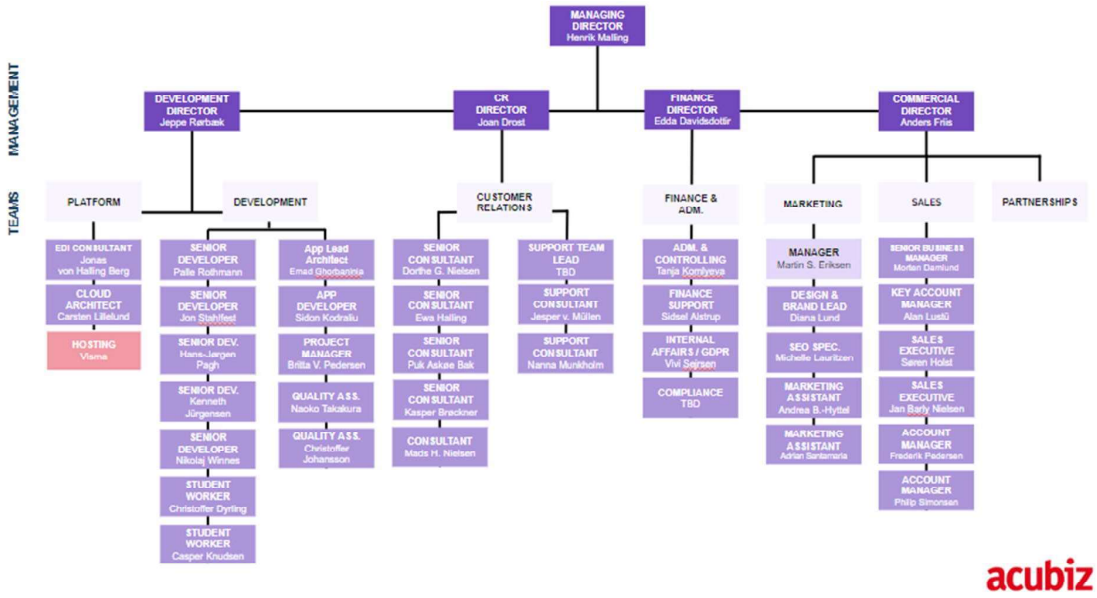
Acubiz Solution (Standard Acubiz) covers the following areas/functionalities:

Function	Description
Credit card integration	Automatic importing of credit card transactions
Travel account integration	Automatic importing of travel card transactions
Cash outlay	Reimbursement of cash outlay
Advances/return advances	Registration of cash advances/return advances
Allowance	Calculation, reporting and reimbursement of daily allowance

Function	Description
Travel orders	Process for prior approval of travel
Export	Option of exporting data for subsequent entry in the finance system and/or payroll system

Visma Acubiz has full control of the development and distribution of this solution. We deliver Acubiz Solution as SAAS, we perform system development of the standard solution, we offer implementation and support to our customers, both public and private, within a wide range of businesses,

Organisational structure



Visma Acubiz's legal owners are Visma Denmark Holding. Acubiz A/S Board consists of 3 Visma employees, of which 1 is Chairman of the Board and further 2 persons are Board Members.

Visma Acubiz's organisation is divided into 9 main areas: "Acubiz Board", "Directors and Management"; "Product and Development", "Operational Excellence and IT-Operation, "Customer Relations", "Marketing and Communications"-" Sales" – "Partnerships" and "Finance and Admin", which all are grouped under a common management with common administration.,

Acubiz Board	Strategy and Business development
Directors and Management	Information Security Board and Product Board
Product and Development	Standard EMS and customization, testing and upgrading of customer's solution
Operational Excellence and IT-Operation	Hosting, Edi, IT administration, internal and customer-related IT operations

Customer Relations	Implementation and training, Service desk and support functions
Marketing and Communication	Digital marketing, Brand and Communication
Sales	Sales and Key account
Partnerships	Sales and 3rd partners (products)
Finance and Admin	Procurement, bookkeeping and other administrative tasks

Acubiz has an Information Security Board (ISB) that meets monthly to deal with security and any security incidents. The committee also assesses whether there are changes in external or internal circumstances that should lead to a reassessment of the preventive or controlling efforts.

Management, Directors, Compliance Manager and DPM are represented in the committee.

Management is responsible for the preparation, maintenance and dissemination of security policy, risk assessment, emergency plans, operating routines and documentation of business processes.

The DPM and Compliance Manager are in charge of the primary contact with accountants and auditors, drive the execution of self-checks, and prepare and update the contingency plan in collaboration with the ISB.

Internal control elements

Control environment

Control environment includes organisation structure, governance, policies and procedures and defines the organisation's general view on internal controls.

The elements in Acubiz's internal control include controls, which may have a radical and permanent effect on Acubiz as a whole or on processes, applications, and transactions patterns. Certain control elements relate to the organisation while others relate to specific procedures or applications

Control activities

Control activities include policies and processes in order to ensure that decisions and measures by the management are implemented in the entity.

Information and communication

This item includes formal, informal and automated systems, which ensure identification, capture and exchange of information so that the employees of the user organization may carry out their work satisfactorily with respect to performance as well as time.

Information and communication are an integral part of Visma Acubiz's internal control system. It covers the processes, which concern identification, collection and exchange of information, form and time frames necessary to manage and control the company's operation. Visma Acubiz identifies processes and reports information through various information systems and dialogue with customers, employees, and other external stakeholders.

Monitoring

This item includes processes to ensure that the quality of the controls is maintained and complies with the quality targets over time.

Acubiz continuously assesses the overall set of controls to secure they sufficiently fulfil the requirements, which we, our customers or the legislation set to us.

Risk assessment

Method for identification and analysis of risks, which may affect Acubiz's goals and activities. It provides a basis for counteracting and handling these risks.

Risk assessment is a critical point in Visma Acubiz's internal control system for handling and continuously assessing risks. The purpose is to identify and classify the risks that may affect the organization's ability to function, see Visma Acubiz's obligations according to Visma Acubiz's General Terms. Visma Acubiz's management is aware of the fact that risks must be reported and treated separately in order to counteract and deal with them, see the stipulated framework.

The challenges faced by Visma Acubiz are therefore assessed and controlled continuously, based upon the result of the risk assessment. If a given risk is identified and found to be significant, separate monitoring is initiated to update the relevant documents, processes and business procedures to ensure mitigation (risk reduction) in relation to the business.

Information security risk assessments are conducted in accordance with recommendations from the Danish Data Protection Agency (Datatilsynet) and ISO/IEC 27001.

Risk assessment model:

Likelihood	Risk levels				
4 - Almost certain	4	8	12	16	
3 - Likely	3	6	9	12	
2 - Possible	2	4	6	8	
1 - Rare	1	2	3	4	
	1 - Minor	2 - Moderate	3 - Major	4 - Severe	Impact

Please refer to section 4 for a description of the specific control objective and control activities.

Complementary controls at the data controllers

Visma's applications were designed on the assumption that certain controls would be implemented and operated effectively by user organisations.

In certain situations, the application of specific controls of the user organisations is necessary to achieve certain control objectives included in this report.

The list below describes additional controls that should be in operation in user organisations to complement the controls at Visma.

The user organisations' auditors should consider whether the following controls have been implemented and operated effectively at the user organisations:

- Controls to provide reasonable assurance that access to Visma's system via interfaces at user locations is restricted to authorised individuals

- Controls to provide reasonable assurance that the user organisation has proper control over the use of IDs and passwords that are used for accessing the solution
- Controls to provide reasonable assurance that the user organisation takes action on access in case of resignations, retirements or job rotations

4. 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 in accordance with the data processing agreement entered into.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
A.1	Written procedures are in place 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.	Checked by way of inspection that formalised procedures are in place to ensure that personal data are only processed according to instructions. Checked by way of inspection 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. Checked by way of inspection that procedures are up to date.	No exceptions noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	Checked by way of inspection that Management ensures that personal data are only processed according to instructions. Checked by way of inspection of a sample of one personal data processing operation that the processing is conducted consistently with instructions.	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	Checked by way of inspection that formalised procedures are in place ensuring verification that personal data are not processed against the Data Protection Regulation or other legislation. Checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is considered to be against legislation.	No exceptions 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	Tests performed by PwC	Result of PwC's tests
B.1	Written procedures are in place which include a requirement that security measures 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.	Checked by way of inspection that formalised procedures are in place to ensure establishment of the security measures agreed. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of one data processing agreement that the security measures agreed have been established.	No exceptions noted.
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the security measures agreed with the data controller.	Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. Checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller.	No exceptions noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data. Checked by way of inspection that antivirus software is up to date.	No exceptions 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	Tests performed by PwC	Result of PwC's tests
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data. Checked by way of inspection that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Checked by way of inspection of a sample of one user's access to systems and databases that such access is restricted to the employees' work-related need.	No exceptions noted.
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data.	Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data.	No exceptions 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	Tests performed by PwC	Result of PwC's tests
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Checked by way of inspection 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. Checked by way of inspection that technological encryption solutions are available and active. Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	No exceptions noted.
B.9	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 set-ups, including disabling of logging ○ Changes in users' system rights ○ Failed attempts to log on to systems, databases or networks Logon data are protected against manipulation and technical errors and are reviewed regularly.	Checked by way of inspection that formalised procedures are in place 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. Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion. Checked by way of inspection of a sample of one day of logging that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents. Checked by way of inspection of a sample of one day of logging that documentation confirms the follow-up performed on activities carried by system administrators and others holding special rights.	No exceptions 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	Tests performed by PwC	Result of PwC's tests
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Checked by way of inspection that formalised procedures are in place for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Checked by way of inspection of a sample of one development or test database that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of a sample of one development or test database 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 exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Checked by way of inspection of one sample that documentation confirms regular testing of the technical measures established.	No exceptions noted.
B.12	Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.	Checked by way of inspection that formalised procedures are in place for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Checked by way of inspection of extracts from technical security parameters and set-ups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.	No exceptions 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	Tests performed by PwC	Result of PwC's tests
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used for processing personal data. Checked by way of inspection of a sample of one employee's access to systems and databases that the user accesses granted have been authorised and that a work-related need exists. Checked by way of inspection of a sample of one resigned or dismissed employee that the employee's access to systems and databases was deactivated or removed in a timely manner. Checked by way of inspection that documentation states that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No exceptions noted.
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	Checked by way of inspection that formalised procedures are in place to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. Checked by way of inspection that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.	No exceptions 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	Tests performed by PwC	Result of PwC's tests
B.15	Physical access security measures 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.	Checked by way of inspection that formalised procedures are in place to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Checked by way of inspection of documentation that only authorised persons have physical access to premises and data centres at which personal data are stored and processed.	No exceptions noted.

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The information 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 information security policy should be updated.	Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year. Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected documentation of Management's assessment that the information security policy generally meets the requirements for security measures and the security of processing in the data processing agreements entered into. Checked by way of inspection of a sample of one data processing agreement that the requirements therein are covered by the requirements of the information security policy for security measures and security of processing.	No exceptions noted.

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • References from former employers • Certificates of criminal record • Diplomas	Checked by way of inspection that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. Checked by way of inspection of a sample of one data processing agreement that the requirements therein for screening employees are covered by the data processor's screening procedures. Checked by way of inspection of one employee appointed during the assurance period that documentation exists of the screening having comprised: • References from former employers • Certificates of criminal record • Diplomas	No exceptions 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.	Checked by way of inspection of one newly appointed employee that the employee has signed a confidentiality agreement. Checked by way of inspection of one newly appointed employee that the employee has been introduced to: • The information security policy • Procedures for processing data and other relevant information.	No exceptions noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	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. Checked by way of inspection of one employee resigned or dismissed that rights have been deactivated or terminated and that assets have been returned.	No exceptions noted.

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Checked by way of inspection that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Checked by way of inspection of one employee resigned or dismissed that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided.	No exceptions 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	Tests performed by PwC	Result of PwC's tests
D.1	Written procedures are in place 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.	Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Checked by way of inspection that procedures are up to date.	No exceptions noted.
D.2	Any specific requirements have been agreed with respect to the data processor's storage periods and deletion routines in the data processing agreements.	Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that personal data are deleted in accordance with the agreed deletion routines.	No exceptions 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.	Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. Checked by way of inspection of one terminated data processing session that documentation states that the agreed deletion or return of data has taken place.	No exceptions noted.

Control objective E:

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
E.1	Written procedures are in place 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.	Checked by way of inspection that formalised procedures are in place for only storing and processing personal data in accordance with the data processing agreements. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that data processing takes place in accordance with the data processing agreement.	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states 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 exceptions noted.

Control objective F:

Procedures and controls are complied with to ensure that only approved subprocessors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.1	Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for subprocessing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for using subprocessors, including requirements for subprocessing agreements and instructions. Checked by way of inspection that procedures are up to date.	No exceptions noted.
F.2	The data processor only uses subprocessors to process personal data that have been specifically or generally approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of subprocessors used. Checked by way of inspection of a sample of one subprocessor from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreement – or otherwise as approved by the data controller.	No exceptions noted.
F.3	When changing the generally approved subprocessors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved subprocessors used, this has been approved by the data controller.	Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the subprocessors used.	No exceptions noted.

Control objective F:

Procedures and controls are complied with to ensure that only approved subprocessors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.4	The data processor has subjected the subprocessor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Checked by way of inspection for existence of signed subprocessing agreements with subprocessors used, which are stated on the data processor's list. Checked by way of inspection of a sample of one subprocessing agreement that it includes the same requirements and obligations as are stipulated in the data processing agreement between the data controller and the data processor.	No exceptions noted.
F.5	The data processor has a list of approved subprocessors disclosing: • Name • Company registration no. • Address • Description of the processing.	Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved. Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor.	No exceptions noted.

Control objective F:

Procedures and controls are complied with to ensure that only approved subprocessors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.6	Based on an updated risk assessment of each subprocessor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the subprocessor.	Checked by way of inspection that formalised procedures are in place for following up on processing activities at subprocessors and compliance with the subprocessing agreements. Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment. Checked by way of inspection of documentation that technical and organisational measures, security of processing at the subprocessors used, third countries' bases of transfer and similar matters are appropriately followed up on. Checked by way of inspection of documentation that information on the follow-up at subprocessors is communicated to the data controller so that such controller may plan an inspection.	No exceptions noted.

Control objective G:

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
G.1	Written procedures are in place which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Checked by way of inspection that procedures are up to date.	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations. Checked by way of inspection of a sample of one data transfer from the data processor's list of transfers that documentation states that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.	No exceptions noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of one data transfer from the data processor's list of transfers that documentation confirms a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place insofar as this was arranged with the data controller.	No exceptions noted.

Control objective H:

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
H.1	Written procedures are in place which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. Checked by way of inspection that procedures are up to date.	No exceptions noted.
H.2	The data processor has established procedures that, insofar as this was agreed, 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.	Checked by way of inspection 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. Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures.	No exceptions noted.

Control objective I:

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	Tests performed by PwC	Result of PwC's tests
I.1	Written procedures are in place which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Checked by way of inspection that procedures are up to date.	No exceptions noted.
I.2	The data processor 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	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. Checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. Checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on in a timely manner.	No exceptions noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a subprocessor.	Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. Made inquiries as to whether personal data breaches have been identified at subprocessors and checked by way of inspection that these breaches are included in the list of security incidents.	No exceptions noted.

Control objective I:

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	Tests performed by PwC	Result of PwC's tests
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of: • The 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.	Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed instructions 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. Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.	No exceptions noted.

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."

Henrik Malling Madsen
Kunde
Serienummer: 6d122022-f082-44a3-a6b9-b10357b25efc
IP: 77.241.xxx.xxx
2024-03-22 12:36:33 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 83.136.xxx.xxx
2024-03-22 12:42:05 UTC