www.pwc.dk

The following is a translation of a Danish original document. Please note that the English translation is provided for convenience only. In case of any discrepancy, the Danish version shall prevail.

Visma Plandisc A/S

Independent auditor's ISAE 3000 assurance report on information security and measures as at 22 February 2024 pursuant to data processing agreements with data controllers

February 2024

pwc

Contents

1 Management's statement

Visma Plandisc A/S processes personal data on behalf of data controllers in accordance with data processing agreements.

The accompanying description has been prepared for data controllers who have used Visma Plandisc A/S's digital solutions and who have 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 Plandisc A/S uses Microsoft, Ipregistry, Safespring AWS, Webhosting and Visma as subprocessors. This report uses the carve-out method and does not comprise control objectives and related controls that the subprocessors perform for Visma Plandisc A/S.

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

Visma Plandisc A/S confirms that:

a) The accompanying description in section 3 fairly presents Visma Plandisc A/S's digital solutions that have processed personal data for data controllers subject to the data protection rules as at 22 February 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Visma Plandisc A/S's digital solutions were designed and implemented, including:

   - The types of services provided, including the type of personal data processed;
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
   - The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects;
   - The procedures ensuring appropriate technical and organisational 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 Visma Plandisc A/S's digital solutions, 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 Visma Plandisc A/S's digital solutions 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 Visma Plandisc A/S's digital solutions 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 22 February 2024. 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.

Aarhus, 28 February 2024
Visma Plandisc A/S

Torben Stigaard
Partner, Managing Director

2 Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures as at 22 February 2024 pursuant to data processing agreements with data controllers

To: Visma Plandisc A/S and data controllers

Scope

We have been engaged to provide assurance about Visma Plandisc A/S's description in section 3 of Visma Plandisc A/S's digital solutions in accordance with data processing agreements with data controllers as at 22 February 2024 (the description) and about the design of controls related to the control objectives stated in the description.

Our report covers whether Visma Plandisc A/S has designed appropriate controls related to the control objectives stated in section 4. The report does not include an assessment of Visma Plandisc 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 Plandisc A/S uses Microsoft, Ipregistry, Safespring AWS, Webhosting and Visma as subprocessors. This report uses the carve-out method and does not comprise control objectives and related controls that the subprocessors perform for Visma Plandisc A/S.

Some of the control objectives stated in Visma Plandisc A/S's description in section 3 can only be achieved if the complementary controls at the data processors are suitably designed together with Visma Plandisc A/S's controls. This report does not comprise the suitability of the design 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 Plandisc A/S's responsibilities

Visma Plandisc 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 Plandisc 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 digital solutions 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 Plandisc 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 Visma Plandisc A/S's digital solutions 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 Visma Plandisc A/S's digital solutions as designed and implemented as at 22 February 2024 and;

b) The controls related to the control objectives stated in the description were suitably designed as at 22 February 2024.

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

Visma Plandisc 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 Visma Plandisc A/S's digital solutions 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.

Aarhus, 28 February 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 this description is to provide Visma Plandisc A/S's customers and their stakeholders (including auditors) with information about compliance with the requirements of the EU General Data Protection Regulation ("the GDPR").

In addition, the purpose of this description is to provide information about the security of processing, technical and organisational measures as well as responsibilities between data controllers (our customers) and Visma Plandisc A/S.

3.1 Nature of processing

The data controller has acquired a licence to Visma Plandisc A/S's digital solutions. Using the solutions, the data controller enters, uploads, imports or otherwise adds data, including personal data, for the purpose of use. In connection with the provision of the solutions, the data processor thus processes personal data on behalf of the data controller in accordance with applicable rules and in accordance with the concluded data processing agreement.

3.2 Personal data

The type of personal data being processed is non-sensitive personal data such as:

1. name
2. phone number
3. email address
4. IP address.

Visma Plandisc A/S processes the categories of personal data on which the data controller has instructed Visma Plandisc A/S and which the data controller has informed about in the data processing agreement. However, using the solution, it is possible for the data controller to entrust Visma Plandisc A/S with the processing of all types of data in view of the data controller's free opportunity to upload or otherwise add data to the solution. If Visma Plandisc A/S learns about the processing of types of personal data that are not specified in the data processing agreement, Visma Plandisc A/S will notify the data controller thereof. However, it is at all times the data controller's responsibility to correctly specify the types of personal data that are comprised by the use of the solution. It is emphasised that Visma Plandisc A/S does not check this, just as Visma Plandisc A/S cannot access the personal data added by the data controller without specific consent.

Categories of data subjects falling within the data processing agreement:

1. The data controller's customers.

Visma Plandisc A/S only processes the data about data subjects on which the data controller has instructed Visma Plandisc A/S and which the data controller has informed about in the data processing agreement. However, using the solution, it is possible for the data controller to entrust someone else with the processing of personal data about all categories of people in view of the data controller's free opportunity to upload or otherwise add data to the solution. If Visma Plandisc A/S learns about the processing of categories of data subjects that are not specified in the data processing agreement, Visma Plandisc A/S will notify the data controller thereof. However, it is at all times the data controller's responsibility to correctly specify the categories of data subjects that are relevant for the data controller's intended use of the solution. It is emphasised that Visma Plandisc A/S does not check this, just as Visma Plandisc A/S cannot access the categories of data subjects added by the data controller without specific consent.

3.3 Instructions from the data controller

1. Visma Plandisc A/S shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. These instructions are stated in the data processing agreement entered into and are specified in detail in the applicable appendices A and C.

2. Visma Plandisc A/S shall inform the data controller immediately if instructions, in Visma Plandisc A/S's opinion, infringe the GDPR or other data protection law of the EU or a Member State.

3. Visma Plandisc A/S has ensured that written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available. A regular – at least annual – assessment is carried out as to whether to update these procedures. Visma Plandisc A/S only performs the processing of personal data stated in the instructions from the data controller.

3.4 Practical measures

The processing of data forms the core of the service we provide to our customers. Thus, our customers' trust and confidence that we can deliver our service in a safe and confidential manner is crucial to the foundation of our business.

We therefore take data protection and the GDPR very seriously and have a constant focus on processing our customers' data securely. This includes continuously improving our technical and organisational security measures.

The following is a non-exhaustive list of our security measures, which are applied by Visma Plandisc A/S and/or purchased from suppliers:

- IT security policy
- Guidelines on human resource security
- Asset management, including control of hand-over and return of assets upon appointment and resignation
- Cryptography
- Supplier relationships and/or plan for supervision of subprocessors
- Management of personal data breaches and incidents
- Ensuring establishment of data processing agreements with subprocessors
- Ensuring that the requirements imposed by law or by customers through contracts and data processing agreements are correspondingly imposed on subprocessors
- Control and updating of risk assessment, policies and procedures
- Ongoing training of employees in the GDPR
- Control of access based on a work-related need.

3.5 Use of subprocessors

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.

When Visma Plandisc A/S engages a subprocessor for carrying out specific processing activities on behalf of the data controller, Visma Plandisc A/S imposes the same data protection obligations as set out in the data processing agreement between Visma Plandisc A/S and the data controller on that subprocessor by

way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the data processing agreement and the GDPR. Visma Plandisc A/S shall therefore be responsible for requiring that the subprocessor at least complies with the obligations to which Visma Plandisc A/S is subject pursuant to the concluded data processing agreement and the GDPR.

Subprocessing agreement(s) and subsequent amendments may be obtained by contacting Visma Plandisc A/S and/or are made available on Visma Plandisc A/S's websites, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in these provisions are imposed on the subprocessor. Provisions on commercial terms that do not affect the legal data protection content of the subprocessing agreement are not made available to the data controller.

3.6 Risk assessment

Visma Plandisc A/S has mapped the risks to the rights of data subjects, including a balancing of the risks against the precautions taken to protect these rights. The actual risk assessment consists of multiple elements, including:

- a mapping of all of the risks involved in the processing and a classification of these risks (scoring, probability and severity)
- an assessment of what constitute appropriate technical and organisational measures to ensure and document compliance with the GDPR.

In Visma Plandisc A/S's own risk assessments, there is not a high risk to the data subjects across all types of data subjects and categories of personal data.

3.7 Control measures

Visma Plandisc A/S has established an annual cycle for systematic measurement and control of the security of processing. Conclusions on controls from the annual cycle are evaluated continuously and at least once a quarter by Management. Required and agreed improvements in this connection are made on a regular basis, and notification of this is found in newsletters to the data controllers. Visma Plandisc A/S has established a number of measures and controls to ensure compliance with the GDPR and the data processing agreements entered into. The established measures and controls comprise the following control objectives:

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.

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.

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.

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.

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.

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.

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.

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.

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.

Also refer to section 4 for a description of the specific control activities.

3.8 Transfer of data

Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

Without documented instructions from the data controller, Visma Plandisc A/S therefore cannot within the framework of the data processing agreement:

a) transfer personal data to a data controller or a data processor in a third country or in an international organisation

b) transfer the processing of personal data to a subprocessor in a third country

c) have the personal data processed by the data processor in a third country.

The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer basis under Chapter V GDPR on which the transfer is based, is set out in appendix C of the data processing agreement.

3.9 The rights of the data subjects

Taking into account the nature of the processing, Visma Plandisc A/S shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that Visma Plandisc A/S, insofar as this is possible, assists the data controller in the data controller's compliance with:

a) the right to be informed when collecting personal data from the data subject

b) the right to be informed when personal data have not been obtained from the data subject

c) the right of access by the data subject

d) the right to rectification

e) the right to erasure ('the right to be forgotten')

f) the right to restriction of processing

g) notification obligation regarding rectification or erasure of personal data or restriction of processing

h) the right to data portability

i) the right to object

j) the right not to be subject to a decision based solely on automated processing, including profiling.

3.10 Handling of personal data breaches

In case of a personal data breach, Visma Plandisc A/S notifies the data controller of the personal data breach without undue delay after having become aware of it.

If possible, the notification to the data controller takes place within 24 hours after Visma Plandisc A/S has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

In accordance with the data processing agreement entered into, Visma Plandisc A/S assists the data controller in notifying the competent supervisory authority of the breach. This means that Visma Plandisc A/S shall assist the data controller in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification of the breach to the competent supervisory authority:

a) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned

b) the likely consequences of the personal data breach

c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Appendix C of the data processing agreement specifies the information to be provided by Visma Plandisc A/S when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

3.11 Record

Visma Plandisc A/S keeps a record of all categories of processing activities carried out on behalf of the data controllers. Visma Plandisc A/S's Management has ensured that the record of categories of processing activities for each data controller contains:

- the name and contact details of the data processor, the data controllers and any representatives and data protection officers of the data controller
- the categories of processing carried out on behalf of each data controller
- where applicable, information on transfer to a third country or an international organisation and documentation of appropriate guarantees
- if possible, a general description of technical and organisational security measures.

Also refer to section 4 for a description of the specific control activities.

3.12 Complementary controls at the data controllers

In addition to the data processor's control measures, it is the data controller's responsibility to ensure the following:

- It is only the data controller who, using the solution, unilaterally enters, uploads, imports or otherwise adds data, including personal data, to the solution. Consequently, the data controller must ensure that the solution is only used according to the types of data subjects and the categories of personal data agreed in the data processing agreement entered into between the parties.
- When requesting support, it is also the responsibility of the data controller to ensure that they only grant access to or share the information required to solve the support request.
- The data controller must ensure that personal data is up to date.
- The data controller must ensure that the necessary legal basis for the processing is in place.
- The data controller must ensure that access and rights to the solution are correct.
- The data controller must ensure that instructions are lawful in relation to the data protection regulation in force at any time and that instructions are appropriate in relation to the agreement entered into on the provision of the digital solution as well as the data processing agreement also entered into in this connection.

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, e.g. in the event of a compromise.	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. TLS encryption in connection with the transmission of emails complies with the Danish Data Protection Agency's requirements in this area.	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. Log 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. Significant vulnerabilities are remediated within a specified and acceptable time frame.	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. Security patches are installed according to the vendor's recommendations and release cycle.	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 and at least every six months, including the continued justification of rights by a work-related need.	Checked by way of inspection that formalised procedures are in place 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	Privileged access to systems and databases processing personal data that involve a high risk for the data subjects is obtained by using as a minimum two-factor authentication or a secured jump host solution.	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.
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 exist 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	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • When the subscription has ended, Plandisc deletes data after 90 days.	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 24 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.