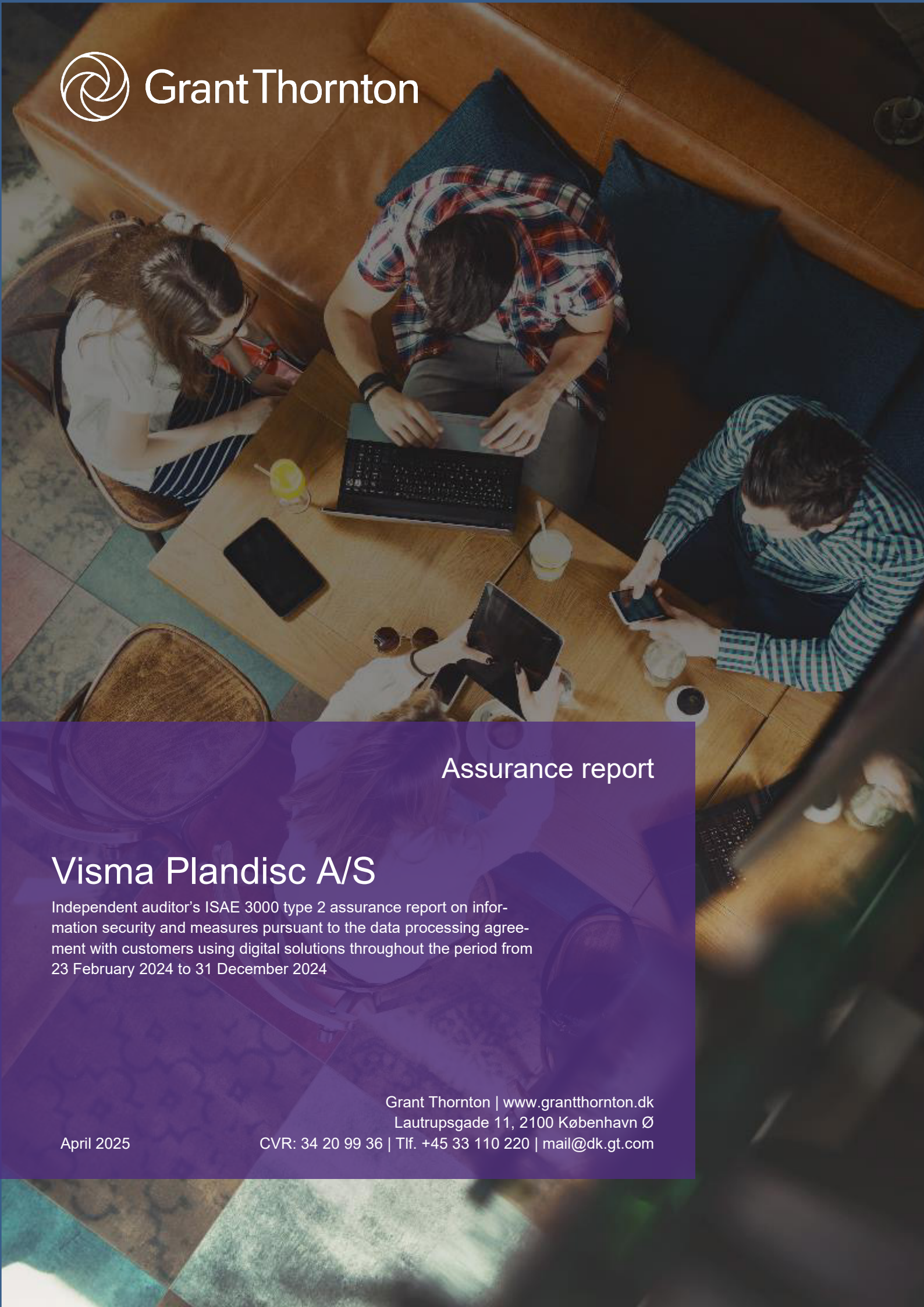

Assurance report

Visma Plandisc A/S

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures pursuant to the data processing agreement with customers using digital solutions throughout the period from 23 February 2024 to 31 December 2024

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

April 2025

Table of Contents

Disclaimer:

The English version of this report was translated from Danish for the convenience of the reader. This translation has not been reviewed or approved by Grant Thornton's auditors. In all legal matters, please refer to the Danish version.

Section 1: Visma Plandisc A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with Visma Plandisc A/S, 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 (hereinafter "the Regulation") have been complied with.

Visma Plandisc A/S uses the following sub-processors, Microsoft Ireland Operations Ltd., Amazon Web Services EMEA SARL, Ipregistry.co, Blue Safespring AB, WebHosting A/S and Visma Data Center. This statement does not include control objectives and related controls at Visma Plandisc A/S' sub-processors. Certain control objectives in the description can only be achieved, if the sub-processor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by sub-processors.

Some of the control areas, stated in Visma Plandisc A/S' description in Section 3 of digital solutions, can only be achieved if the complementary user entity controls with the data controllers are suitably designed and operationally effective with Visma Plandisc A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Visma Plandisc A/S confirms that:

a) The accompanying description, Section 3, fairly presents how Visma Plandisc A/S has processed personal data on behalf of data controllers throughout the period from 23 February 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Visma Plandisc A/S' processes and controls related to data protection 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 safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
   - Controls that we, in reference to the scope of Visma Plandisc A/S, have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Includes relevant information about changes in the data processor's digital solutions in the processing of personal data during the period from 23 February 2024 to 31 December 2024;

(iii) Does not omit or distort information relevant to the scope of digital solutions 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 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, in our view, suitably designed and operated effectively throughout the period from 23 February 2024 to 31 December 2024, if relevant controls with sub-processors were operationally effective and data controller has performed the complementary user entity controls, assumed in the design of Visma Plandisc A/S' controls during the period from 23 February 2024 to 31 December 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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 23 February 2024 to 31 December 2024.

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

Aarhus, 25 April 2025
Visma Plandisc A/S

Torben Stigaard
Partner, Managing Director

Section 2: Independent auditor's assurance report with reasonable assurance on information security and measures pursuant to data processing agreements with data controllers during the period from 23 February 2024 to 31 December 2024

To: Visma Plandisc A/S and their customers

Scope

We were engaged to provide assurance about a) Visma Plandisc A/S' description, Section 3 of digital solutions in accordance with the data processing agreement with data controllers throughout the period from 23 February 2024 to 31 December 2024 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the Description.

Visma Plandisc A/S uses the following sub-processors: Microsoft Ireland Operations Ltd., Amazon Web Services EMEA SARL, Ipregistry.co, Blue Safespring AB, WebHosting A/S and Visma Data Center. This statement does not include control objectives and related controls at Visma Plandisc A/S' sub-processors. Certain control objectives in the description can only be achieved if the sub-processor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by sub-processor.

Some of the control objectives stated in Visma Plandisc A/S' description in Section 3 of digital solutions, can only be achieved if the complementary user entity controls with the data controller have been appropriately designed and operating effectively with the controls with Visma Plandisc A/S. The report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Our opinion is based on reasonable assurance.

Visma Plandisc A/S' responsibilities

Visma Plandisc A/S is responsible for: preparing the Description and the accompanying statement, Section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and for the design and implementation of operationally effective controls, to achieve the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and 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' Description and on the design and operational effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

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

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its digital solutions and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

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

Limitations of controls at a data processor

Visma Plandisc A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of 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 personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

(a) the description fairly presents how the IT general controls in relation to Visma Plandisc A/S' digital solutions were designed and implemented throughout the period from 23 February 2024 to 31 December 2024.

(b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 23 February 2024 to 31 December 2024 in all material respects, and

(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period 23 February 2024 to 31 December 2024.

Description of tests of controls

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

Intended users and purpose

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

Copenhagen, 25 April 2025

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Partner, CISA, CISM

Section 3: Visma Plandisc A/S' description of processing activity for the supply of digital solutions

The purpose of this description is to provide information for Visma Plandisc A/S' customers and their stakeholders (including auditors) about compliance with the content of EU's General Data Protection Regulation ("GDPR").

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

The purpose of the data processor's processing of personal information on behalf of the data controller

The purpose of processing the data controller's personal information is to fulfil the agreement between the data processor and the data controller on delivery of solutions and services.

The purpose of the data controller's solutions and/or services include:

- **Plandisc Private Cloud:** Plandisc is a digital annual wheel, helping companies, organisations and educational institutions to plan, coordinate and visualise their activities over a period of time. With Plandisc the users can have a complete overview of important deadlines, tasks and strategic goals in a circular diary, supporting collaboration across teams.

The Private Cloud version uses the sub-processors:
Webhosting.dk, Azure (Microsoft) and Safespring.

- **Plandisc Public Cloud:** Plandisc is a digital annual wheel, helping companies, organisations and educational institutions to plan, coordinate and visualise their activities over a period of time. With Plandisc the users can have a complete overview of important deadlines, tasks and strategic goals in a circular diary, supporting collaboration across teams.

The Public Cloud version uses the sub-processors:
Webhosting.dk, Azure (Microsoft), Amazon AWS og Ipregistry

The nature of the processing

The data controller has acquired a license for Visma Plandisc A/S' digital solutions, where the data controller, by using the solutions, enters, uploads, imports, or otherwise adds data, including personal data, to the solutions for the purpose of use. In connection with the delivery of the solutions, the data processor thus processes personal data on behalf of the data controller according to applicable regulations and in accordance with the signed data processing agreement.

Categories of personal data and categories of data subjects

The type of personal data being processed are sensitive personal information, such as:

1. Name
2. Telephone number
3. E-mail address
4. EIP-address

Visma Plandisc A/S processes the categories of personal data, as instructed by the data controller and described in the data processing agreement. When using the solution, there is, however, the possibility for the data controller to entrust the processing of all types of data to Visma Plandisc A/S, given the data controller's free ability to upload or otherwise add data to the solution.

If Visma Plandisc A/S becomes aware of the processing of types of personal data that are not anticipated in the data processing agreement, Visma Plandisc A/S will notify the data controller thereof. However, it is always the responsibility of the data controller to correctly specify the types of personal data that the use of the solution encompasses. It is emphasised that Visma Plandisc A/S does not conduct checks in this regard, nor can Visma Plandisc A/S access the personal data added by the data controller without separate consent.

Categories of data subjects included in the data processing agreement:

- The data controllers' customers

Visma Plandisc A/S only processes data about the data subjects as instructed by data controller and described the data processing agreement. However, when using the solution, the data controller has the possibility to entrust the processing of personal data concerning all categories of persons, given the data controller's free ability to upload or otherwise add data to the solution. If Visma Plandisc A/S becomes aware of the processing of categories of data subjects not anticipated in the data processing agreement, Visma Plandisc A/S will notify the data controller thereof. However, it is always the responsibility of the data controller to correctly specify the categories of data subjects relevant to the data controller's intended use of the solution. It is emphasised that Visma Plandisc A/S does not conduct checks in this regard, nor can Visma Plandisc A/S access the categories of data subjects added by the data controller without separate consent.

Instructions from the data controller

1. Visma Plandisc A/S may only process personal data according to documented instructions from the data controller, unless required by EU law or the national law of the member states to which the data processor is subject. This instruction is outlined in the entered data processing agreement and is further specified in the applicable appendices A and C
2. Visma Plandisc A/S will immediately notify the data controller if an instruction, in their opinion, is in violation of this regulation or data protection provisions in other EU law or the national law of the member states
3. Visma Plandisc A/S has ensured that written procedures are in place, including requirements that personal data may only be processed when there is an instruction. These procedures are continuously assessed – and at least once a year – to determine whether updates are necessary. Visma Plandisc A/S only performs the processing of personal data as described in the instructions from the data controller.

Practical measures

The processing of data is the core of the service we provide to our customers. Therefore, our customers' trust and confidence in our ability to deliver our services securely and confidentially is of utmost importance to our business foundation. We take data protection and GDPR very seriously and maintain a continuous focus on processing our customers' data securely, including through ongoing improvements to our technical and organisational security measures. The following is a non-exhaustive list of our security measures, which are carried out either by Visma Plandisc A/S and/or purchased from suppliers:

- IT security policy
- Employee security guidelines
- Asset management, including control of delivery and return of assets upon hiring and termination
- Cryptography
- Supplier relationships and/or supervision plan with sub-processors
- Managing personal data breaches and incident management
- Ensure the establishment of data processing agreements with sub-processors
- Ensure that the requirements imposed by legislation or by customers through contracts and data processing agreements are similarly imposed on sub-processors
- Monitoring and updating risk assessment, policies and procedures
- Ongoing GDPR training of employees
- Access management, based on a work-related need.

The use of sub-processors

Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by monitoring their technical and organisational measures to protect the rights of data subjects and the processing of personal data, ensures a reassuring level of processing security

When Visma Plandisc A/S use a sub-processor in connection with performing specific processing activities on behalf of the data controller, Visma Plandisc A/S ensures, through a contract or other legal document in accordance with EU law or the national law of the member states, to impose on the sub-processor the same data protection obligations as those outlined in the data processing agreement between Visma Plandisc A/S and the data controller. This particularly provides the necessary guarantees that the sub-processor will implement the technical and organisational measures in such a way that the processing complies with the requirements of the data processing agreement and the General Data Protection Regulation (GDPR). Visma Plandisc A/S is therefore responsible for requiring that the sub-processor, as a minimum, complies with Visma Plandisc A/S' obligations under the entered data processing agreement and the GDPR.

Sub-processing agreements and any subsequent amendments thereto, are available on the websites belonging to Visma Plandisc A/S, thereby allowing the data controller to ensure that equivalent data protection obligations as stipulated by these provisions are imposed on the sub-processor. Provisions regarding commercial terms that do not affect the data protection content of the sub-processing agreement are not made available to the data controller

Risk assessment

Visma Plandisc A/S has conducted a mapping of the risks to the rights of data subjects, including an assessment of these risks in relation to the measures taken to protect these rights. The risk assessment itself consists of several parts, including:

- Mapping of all risks associated with processing and categorisation of these risks (including scoring of likelihood and severity)
- Assesment of which technical and organisational measures, that will be appropriate to ensure compliance with the Data Protection Regulation and the ability to document this.

In the risk assessments, prepared by Visma Plandisc A/S, there is no high risk for the data subjects, across all types of data subjects and categories of personal data.

Control measures

Visma Plandisc A/S has established a systematic process, called an annual wheel, to measure and control processing security. The results of these controls are continuously assessed and at least quarterly by management. Any necessary improvements decided upon based on the evaluation are implemented continuously, and the data controllers are informed of the changes via newsletters.

Visma Plandisc A/S has established a series of measures and controls to ensure compliance with the General Data Protection Regulation (GDPR) and the entered data processing agreements. The specific control objectives include:

- Control objective A
  - Procedures and controls are followed to ensure that instructions concerning personal data processing is complied with according to the signed data processing agreement.
- Control objective B
  - Procedures and controls are followed ensuring that the data processor has implemented technical measures to ensure relevant processing security.
- Control objective C
  - Procedures and controls are followed ensuring that the data processor has implemented organisational measures to ensure relevant processing security.

- Control objective D
    - Procedures and controls are followed ensuring that personal data can be deleted or returned, should this be agreed with the data controller.
- Control objective E
    - Procedures and controls ensuring that the data processor stores personal data according to the agreement with the data controller.
- Control objective F
    - Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by monitoring their technical and organisational measures to protect the rights of data subjects and the processing of personal data, ensures a reassuring level of processing security
- Control objective G
    - Procedures and controls are followed to ensure that the data processor only transfers personal data to third countries or international organisations in accordance with the agreement with the data controller and based on a valid transfer basis..
- Control objective H
    - Procedures and controls are followed to ensure that the data processor can assist the data controller with the delivery, correction, deletion, or restriction of information regarding the processing of personal data to the data subject.
- Control objective I
    - Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the signed data processing agreement.

Please refer to Section 4, where the specific control activities are described.

Transfer of personal data

Any transfer of personal data to third countries or international organisation can only be done by the data processor based on documented instructions from the data controller and must always be in compliance with the Data Protection Regulation's Chapter V.

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

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

b. leave processing of personal data to a sub-processor in a third country

c. process personal data in a third country

The data controller's instructions regarding the transfer of personal data to a third country, including any transfer basis in Chapter V of the General Data Protection Regulation (GDPR) on which the transfer is based, are specified in Appendix C, C.6 of the data processing agreement

The data subjects' rights

Visma Plandisc A/S assists, taking into account the nature of the processing, as much as possible the data controller by means of appropriate technical and organisational measures in fulfilling the data controller's obligation to respond to requests for exercising the data subjects' rights as set out in Chapter III of the General Data Protection Regulation (GDPR).

This means that Visma Plandisc A/S, as much as possible, assists the data controller in ensuring compliance with:

a) **Duty of disclosure:** Upon gathering of personal data from the data subject.
b) **Duty of disclosure:** If personal data are not gathered from the data subject
c) **The right to access:** The right to access the processed personal data
d) **The right to rectification: T**he right to have incorrect personal data rectified
e) **The right to deletion (the right to be forgotten):** The right to have personal data deleted
f) **The right to restrict processing:** The right to restrict the processing of personal data
g) **The right to be informed:** The right to be informed about correction or deletion of personal data or restriction of the processing
h) **The right to data portability:** The right to have personal data transferred to another data controller.
i) **The right to object:** The right to object to processing of personal data
j) **The right to not being the object of automated decision making:** The right to not being the object of decisions, solely based on automated processing, including profiling.

Managing personal data breaches

Visma Plandisc A/S notifies the data controller without undue delay after becoming aware of a personal data security breach.

The data controller is notified, if possible, no later than 24 hours after Visma Plandisc A/S has become aware of the breach, so that the data controller can fulfil its obligation to report the personal data security breach to the competent supervisory authority, in accordance with Article 33 of the General Data Protection Regulation (GDPR).

In accordance with the signed data processing agreement, Visma Plandisc A/S assists the data controller in making the notification of the breach to the competent supervisory authority. This means that Visma Plandisc A/S must assist in providing the following information, which according to Article 33, paragraph 3, must be included in the data controller's notification of the breach to the competent supervisory authority:

a) The nature of the breach, including, if possible, the categories and approximate number of affected data subjects, as well as the categories and approximate number of affected personal data records.

b) The likely consequences of the personal data security breach.

c) The measures that the data controller has taken or proposes to take to address the personal data security breach, including any actions to mitigate its possible adverse effects

Appendix C of the data processing agreement contains detailed information that Visma Plandisc A/S provides in connection with its assistance to the data controller in fulfilling its obligation to report personal data security breaches to the competent supervisory authority.

Record

Visma Plandisc A/S keeps a record of all categories of processing activities, performed on behalf of the data controllers.

Visma Plandisc A/S has ensured that the record of categories of processing activities with the individual data controller, includes:

- Name and contact information of the data processor, that data controllers as well as their possible representatives and data protection officers.
- The categories of processing, performed on behalf of the individual data controller.
- Information about transfer to a third country or an international organisation, if relevant, as well as documentation of adequate guarantees.
- A general description of the technical and organisational measures, if possible.

Complementary user entity controls with the data controllers

Apart from the data processor's control measures, the data controller is responsible for ensuring the following:

- Correct use of the solution: The data controller, who records, uploads, imports or in another way adds data to the solution, must ensure, that this happens according to the agreed types of data subjects and categories of personal data, specified in the data processing agreement.
- Support requests: Upon requests for support, it is the data controller's responsibility to ensure that only the information necessary to solve the support request is shared or given access to.
- Updating personal data: The data controller must ensure, that the processed personal data always are updated and correct.
- Lawful processing: The data controller must ensure that the necessary legal basis for processing is in place.
- Correct accesses and rights: The data controller must ensure that accesses and rights to the solution are correct and according to the signed agreement.
- Instruction legality: The data controller must ensure that the issued instruction is lawful under applicable data protection legislation and appropriate in relation to the subscription agreement and data processing agreement.
- Deletion of data: The data controller is familiar with the solution for deletion of data, and it is expected that the data controller will handle the deletion or withdrawal of data, including personal data. Visma Plandisc A/S can, upon request, carry out deletion as described in the data processing agreement.
- Requests from data subjects: The solution supports the data controller's responsibilities while handling requests from data subjects. The data controller can thus fulfil these requests themselves, but Visma Plandisc A/S acknowledges its duty to assist when needed.

Section 4: Control objectives, controls, tests, and results hereof

We conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our test of the functionality has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls; we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 23 February 2024 to 31 December 2024.

Our statement, does not apply to controls, performed at Visma Plandisc A/S' sub-processors.

Further, controls performed at the data controller are not included in this statement.

We performed our test of controls at Visma Plandisc A/S by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Visma Plandisc A/S. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2.

Articles and points about main areas are written in bold.

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*New scope compared to ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*New scope compared to ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*New scope compared to ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Control objective A - Instructions regarding processing of personal data

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing. We have inspected that procedures are up to date.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected that management ensures that personal data are only processed according to instructions. We have inspected that a sample of personal data processing operations are conducted consistently with instructions.	No deviations 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.	We have inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. We have inspected that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation.	We have been informed that the data processor has not received instructions, that in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions. No deviations noted.

Control objective B - Technical measures

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed. We have inspected that procedures are up to date. We have, by sample test, inspected that the safeguards agreed in the data processing agreements, have been established.	No deviations 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 safeguards agreed with the data controller.	We have inspected that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. We have inspected that the risk assessment performed is up to date and comprises the current processing of personal data. We have, by sample test, inspected that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. We have, by sample test, inspected that the data processor has implemented the safeguards agreed with the data controller.	No deviations 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.	We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed. We have inspected that antivirus software is up to date.	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	We have inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. We have inspected that the firewall has been setup and is up to date.	No deviations noted.

Control objective B - Technical measures

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. We have inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data. We have inspected that access is restricted to the employees' work-related need for a sample of users' access to systems and databases.	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. We have, by sample test, inspected that a sample of alarms were followed up on and that the data controllers were informed thereof as appropriate.	No deviations noted.

Control objective B - Technical measures

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have inspected that technological encryption solutions have been available and active throughout the assurance period. We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by e-mail.	No deviations noted.
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation, technical errors and are reviewed regularly.	We have inspected that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs. We have inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. We have inspected that user activity data collected in logs are protected against manipulation or deletion. We have, by sample test, inspected that the content of a sample of log files is as expected compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents. We have, by sample test, inspected that documentation exists for the follow-up performed for activities carried by system administrators and others holding special rights.	No deviations noted.

Control objective B - Technical measures

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form.	We have inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. We have, by sample test, inspected that documentation exists regarding regular testing of the technical measures established. We have inspected that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	No deviations noted.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inspected that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches. We have, by sample test, inspected that changes in systems, databases and networks are managed according to the procedure.	No deviations noted.
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.	We have inspected that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data. We have inspected, that documentation exists of regular – and at least twice a year – assessment and approval of user accesses granted.	No deviations noted.

Control objective B - Technical measures

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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.	We have inspected that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. We have inspected that users' access to processing personal data that involve a high risk for the data subjects can only take place by using two-factor authentication.	No deviations noted.
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	We have inspected that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. We have inquired whether only authorised employees have had access to premises at which personal data are processed. We have inspected, that internal control of physical access security for premises, at which data are stored and processed, has been carried out. We have inspected that review of test results related to physical security in third party assurance reports from sub-processors used for hosting, storage and processing of personal data, has been carried out.	No deviations noted.

Control objective C - Organisational measures

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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 IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists that Management has considered and approved within the past year. We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have inspected documentation of management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. We have, by sample test, inspected that there is documentation that the testing of new employees during the audit period has included: • References from previous employment • Criminal record	No deviations noted.

Control objective C - Organisational measures

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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.	We have, by sample test, inspected that employees appointed during the assurance period have signed a confidentiality agreement. We have, by sample test, inspected that employees appointed during the assurance period have been introduced to: • Information security policy. • Procedures for processing data and other relevant information.	No deviations 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.	We have 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. We have, by sample test, inspected that rights have been deactivated or terminated and that assets have been returned for employees resigned or dismissed during the assurance period.	No deviations noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	We have inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We have, by sample test, inspected that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality for employees terminated during the assurance period.	No deviations 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.	We have inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No deviations noted.

Control objective D - Return and deletion of personal data

Procedures and controls are complied with to ensure that personal data are deleted or returned if arrangements are made with the data controller to this effect.

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. We have inspected that the procedures are up to date.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. We have, by sample test, inspected that there is documentation confirming that the agreed deletion or return of data has been carried out for data processing activities terminated during the declaration period.	No deviations noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. We have, by sample test, inspected that documentation exists that the agreed deletion or return of data has taken place for terminated data processing sessions during the assurance period.	No deviations noted.

Control objective E – Storage of personal data

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.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. We have inspected that the procedures are up to date.	No deviations 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.	We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions. We have, by sample test, inspected that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No deviations noted.

Control objective F – Use of sub-processors

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
F.1	Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for using sub-processors, including requirements for sub-data processing agreements and instructions. We have inspected that procedures are up to date.	No deviations noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of sub-processors used. We have, by sample test, inspected that documentation exists that the processing of data by the sub-processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No deviations noted.
F.3	When changing the generally approved sub-processors 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 sub-processors used, this has been approved by the data controller.	We have inspected that formalised procedures are in place for informing the data controller when changing the sub-processors used. We have inspected documentation that the data controller was informed when changing the sub-processors used throughout the assurance period.	We have been informed, that no changes have occurred in the use of sub-processors during the audit period. No deviations noted.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inspected for existence of signed sub-data processing agreements with sub-processors used, which are stated on the data processor's list. We have, by sample test, inspected that sub-data processing agreements include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.

Control objective F – Use of sub-processors

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

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
F.5	The data processor has a list of approved sub-processors.	We have inspected that the data processor has a complete and updated list of sub-processors used and approved of. We have inspected that, as a minimum, the list includes the required details about each sub-processor.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-processor 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 sub-processor.	We have inspected that formalised procedures are in place for following up on processing activities at sub-processors and compliance with the sub-data processing agreements. We have inspected documentation that each sub-processor and the current processing activity at such processor are subjected to risk assessment. We have inspected documentation that technical and organisational measures, security of processing at the sub-processors used, third countries' bases of transfer and similar matters are appropriately followed up on. We have inspected documentation that information on the follow-up at sub-processors is communicated to the data controller so that such controller may plan an inspection.	No deviations noted.

Control objective G – Transfer of personal data to third countries

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.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
G.1	Written procedures exist 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.	We have inspected that formalised procedures exist 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. We have inspected that procedures are up to date.	No deviations noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	We have inspected that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations. We have inquired whether the data processor has transferred personal data to third countries or international organisations.	We have been informed, that personal data are not being transferred to third countries or international organisations. No deviations 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.	We have inspected that formalised procedures are in place for ensuring a valid basis of transfer. We have inspected that procedures are up to date. We have inquired whether the data processor has transferred personal data to third countries or international organisations.	We have been informed, that personal data are not being transferred to third countries or international organisations. No deviations noted.

Control objective H – Rights of the data subjects

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.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
H.1	Written procedures exist 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.	We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that procedures are up to date.	No deviations noted.
H.2	The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects.	We have inspected that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. We have inspected documentation that the systems and databases used support the performance of the relevant detailed procedures.	We have been informed that the data processor has not received any requests from the data controller related to the data subjects' rights. No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.1	Written procedures exist 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.	We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that procedures are up to date.	No deviations noted.
I.2	The data processor has established controls for identification of possible personal data breaches.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. We have inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. We have inspected documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on, on a timely basis.	No deviations noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-processor.	We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. We have inquired whether any personal data breaches have occurred during the audit period.	We have been informed, that no personal data breaches have occurred during the audit period. No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.

No.	*Visma Plandisc A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • Nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	We have inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. We have inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	No deviations noted.