plandisc

Data Processing Agreement

Data Processing Agreement

pursuant to Article 28(3) of Regulation (EU) 2016/679 (the General Data Protection Regulation) concerning the Data Processor's processing of personal data

between

[Company name]
CVR: [ ]

hereinafter referred to as the "Data Controller"

og

Visma Plandisc A/S
CVR: 37204854
Axel Kiers Vej 5A 8270 Højbjerg
Denmark

hereinafter referred to as the "Data Processor"

each individually a "Party" and together the "Parties"

HAVE AGREED on the following standard contractual clauses (the "Clauses") in order to ensure compliance with the General Data Protection Regulation and to ensure the protection of privacy and the fundamental rights and freedoms of natural persons.

Contents

1. Preamble

1. These Clauses set out the rights and obligations of the Data Processor when processing personal data on behalf of the Data Controller.

2. These Clauses have been drafted to ensure the Parties' compliance with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation).

3. In connection with the provision of licences for the Data Processor's solution(s) and service(s), the Data Processor processes personal data on behalf of the Data Controller in accordance with these Clauses.

4. These Clauses shall prevail over any corresponding provisions contained in other agreements entered into between the Parties.

5. Five (5) appendices are attached to and form an integral part of these Clauses.

6. Appendix A contains further details regarding the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects, and the duration of the processing.

7. Appendix B contains the Data Controller's terms governing the Data Processor's use of sub-processors, as well as a list of sub-processors approved by the Data Controller.

8. Appendix C contains the Data Controller's instructions regarding the Data Processor's processing of personal data, a description of the technical and organisational security measures that the Data Processor shall, as a minimum, implement, and the manner in which supervision of the Data Processor and any sub-processors is carried out.

9. Appendix D contains provisions relating to other activities not covered by these Clauses.

10. Appendix E contains a description of the data processing chain.

11. These Clauses and the associated appendices shall be retained in writing, including in electronic form, by both Parties.

12. These Clauses do not relieve the Data Processor of any obligations imposed on the Data Processor under the General Data Protection Regulation or any other applicable legislation.

2. The Data Controller's Rights and Obligations

1. The Data Controller shall be responsible for ensuring that the processing of personal data is carried out in compliance with the General Data Protection Regulation (see Article 24 of the Regulation), data protection provisions laid down in other EU law or in the national law of the Member States, and these Clauses.

2. The Data Controller has the right and the obligation to decide for which purpose(s) and by which means the processing of personal data may be carried out.

3. The Data Controller shall be responsible, inter alia, for ensuring that there is a lawful basis for the processing of personal data which the Data Processor is instructed to carry out.

3. Processing on Documented Instructions

1. The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union law or Member State law to which the Data Processor is subject. Such instructions shall be specified in Appendices A and C. Subsequent instructions may also be given by the Data Controller while the processing of personal data is ongoing; however, such instructions shall always be documented and retained in writing, including in electronic form, together with these Clauses.

2. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes this Regulation or data protection provisions laid down in other Union law or in the national law of the Member States.

4. Confidentiality

1. The Data Processor shall grant access to personal data processed on behalf of the Data Controller only to persons who are subject to the Data Processor's authority and who have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons granted access shall be reviewed on an ongoing basis. Based on such review, access to personal data shall be revoked where such access is no longer necessary, and the personal data shall thereafter no longer be available to such persons.

2. Upon request from the Data Controller, the Data Processor shall be able to demonstrate that the persons subject to the Data Processor's authority are subject to the above-mentioned duty of confidentiality.

5. Security of Processing

1. Article 32 of the General Data Protection Regulation provides that the Data Controller and the Data Processor shall, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The Data Controller shall assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate such risks. Depending on their relevance, such measures may include:

a. pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
c. the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. Pursuant to Article 32 of the Regulation, the Data Processor shall also, independently of the Data Controller, assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate such risks. For the purposes of such assessment, the Data Controller shall provide the Data Processor with the necessary information enabling the Data Processor to identify and assess such risks.

3. Furthermore, the Data Processor shall assist the Data Controller in complying with its obligations under Article 32 of the Regulation, inter alia by making available to the Data Controller the necessary information regarding the technical and organisational security measures already implemented by the Data Processor pursuant to Article 32 of the Regulation, as well as any other information required to enable the Data Controller to comply with its obligations under Article 32.

   Where, following the Data Controller's assessment, the mitigation of the identified risks requires the implementation of additional measures beyond those already implemented by the Data Processor, the Data Controller shall specify such additional measures to be implemented in Appendix C.

6. Use of Sub-processors

1. The Data Processor shall comply with the conditions set out in Article 28(2) and (4) of the General Data Protection Regulation when engaging another processor (a sub-processor).

2. Accordingly, the Data Processor shall not engage a sub-processor for the performance of these Clauses without the prior general written authorisation of the Data Controller.

3. The Data Processor has the Data Controller's general authorisation to engage sub-processors. The Data Processor shall inform the Data Controller in writing of any intended changes concerning the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the relevant sub-processor(s). Longer notice periods for specific processing activities may be specified in Appendix B. The list of sub-processors already approved by the Data Controller is set out in Appendix B.

4. Where the Data Processor engages a sub-processor in connection with the performance of specific processing activities on behalf of the Data Controller, the Data Processor shall, by way of a contract or other legal act under Union law or Member State law, impose on the sub-processor the same data protection obligations as those set out in these Clauses. In particular, the Data Processor shall ensure that sufficient guarantees are provided that the sub-processor will implement appropriate technical

and organisational measures in such a manner that the processing will meet the requirements of these Clauses and the General Data Protection Regulation.

The Data Processor shall therefore be responsible for ensuring that the sub-processor, as a minimum, complies with the obligations imposed on the Data Processor under these Clauses and the General Data Protection Regulation.

5. Upon the Data Controller's request, copies of sub-processing agreements and any subsequent amendments thereto shall be provided to the Data Controller, thereby enabling the Data Controller to verify that equivalent data protection obligations to those contained in these Clauses have been imposed on the sub-processor. Provisions relating to commercial terms that do not affect the data protection content of the sub-processing agreement shall not be disclosed to the Data Controller.

6. Where a sub-processor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of the sub-processor's obligations. This shall be without prejudice to the rights of data subjects under the General Data Protection Regulation, in particular Articles 79 and 82, against the Data Controller and the Data Processor, including the sub-processor.

7. Transfers to Third Countries or International Organisations

1. Any transfer of personal data to third countries or international organisations shall only be carried out by the Data Processor on the basis of documented instructions from the Data Controller and shall in all cases be carried out in compliance with Chapter V of the General Data Protection Regulation.

2. Where a transfer of personal data to third countries or international organisations which the Data Processor has not been instructed by the Data Controller to carry out is required under Union law or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of such legal requirement prior to processing, unless such law prohibits such notification on important grounds of public interest.

3. Accordingly, without documented instructions from the Data Controller, the Data Processor shall not, within the framework of these Clauses:

    a. transfer personal data to a data controller or data processor in a third country or an international organisation;
    b. entrust the processing of personal data to a sub-processor located in a third country;
    c. process personal data in a third country.

4. The Data Controller's instructions regarding the transfer of personal data to a third country, including any applicable transfer mechanism under Chapter V of the General Data Protection Regulation on which the transfer is based, shall be specified in Appendix C.6.

5. These Clauses shall not be confused with standard contractual clauses as referred to in Article 46(2)(c) and (d) of the General Data Protection Regulation, and these Clauses shall not constitute a valid transfer mechanism for the transfer of personal data pursuant to Chapter V of the General Data Protection Regulation.

8. Assistance to the Data Controller

1. Taking into account the nature of the processing, the Data Processor shall, to the extent possible, assist the Data Controller by appropriate technical and organisational measures in fulfilling the Data Controller's obligation to respond to requests for exercising the data subjects' rights laid down in Chapter III of the General Data Protection Regulation.

   This includes that the Data Processor shall, to the extent possible, assist the Data Controller in ensuring compliance with the following obligations and rights:

   a. the duty to provide information where personal data are collected from the data subject;
   b. the duty to provide information where personal data have not been obtained from the data subject;
   c. the right of access;
   d. he right to rectification;
   e. the right to erasure ("the right to be forgotten");
   f. the right to restriction of processing;
   g. the obligation to notify in connection with 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.

2. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 6.3, the Data Processor shall further, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller with:

   a. the Data Controller's obligation to notify a personal data breach to the competent supervisory authority, the Danish Data Protection Agency, without undue delay and, where feasible, no later than twenty-four (24) hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the Data Controller's obligation to communicate the personal data breach to the data subject without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the Data Controller's obligation, prior to processing, to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the Data Controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

3. The Parties shall specify in Appendix C the necessary technical and organisational measures by which the Data Processor shall assist the Data Controller, as well as the extent and scope of such assistance. This shall apply to the obligations set out in Clauses 9.1 and 9.2.

9. Notification of a Personal Data Breach

1. The Data Processor shall notify the Data Controller without undue delay after having become aware that a personal data breach has occurred.

2. Where possible, the Data Processor's notification to the Data Controller shall be made no later than twenty-four (24) hours after the Data Processor has become aware of the breach, so as to enable the Data Controller to comply with its obligation to notify the personal data breach to the competent supervisory authority pursuant to Article 33 of the General Data Protection Regulation.

3. In accordance with Clause 9.2(a), the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority. This means that the Data Processor shall assist in providing the information listed below, which, pursuant to Article 33(3) of the General Data Protection Regulation, must be included in the Data Controller's notification of the personal data breach to the competent supervisory authority:

    a. the nature of the personal data breach, 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 Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The Parties shall specify in Appendix C the information which the Data Processor shall provide in connection with its assistance to the Data Controller in fulfilling the Data Controller's obligation to notify personal data breaches to the competent supervisory authority.

10. Deletion and Return of Data

1. Upon termination of the Data Processor's services relating to the processing of personal data, the Data Processor shall be obliged to delete all personal data processed on behalf of the Data Controller and to confirm to the Data Controller that such data has been deleted, unless the Data Controller instructs the Data Processor otherwise or unless Union law or Member State law requires the storage of the personal data.

11. Audit, Including Inspections

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and these Clauses, and shall allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor authorised by the Data Controller.

2. The procedures applicable to audits, including inspections, carried out by the Data Controller in relation to the Data Processor and any sub-processors are further specified in Appendices C.7 and C.8.

3. The Data Processor shall be obliged to grant supervisory authorities which, pursuant to applicable law, have access to the facilities of the Data Controller or the Data Processor, or representatives acting on behalf of such supervisory authorities, access to the Data Processor's physical premises upon presentation of appropriate identification.

12. The Parties' Agreement on Other Matters

1. The Parties may agree on other provisions relating to the service in connection with the processing of personal data, including, for example, provisions on liability, provided that such provisions do not directly or indirectly conflict with these Clauses or undermine the fundamental rights and freedoms of data subjects as set out in the General Data Protection Regulation.

13. Entry into Force and Termination

1. These Clauses shall enter into force on the date of signature by both Parties.

2. Either Party may request that these Clauses be renegotiated if changes in legislation or deficiencies in the Clauses give rise to such need.

3. These Clauses shall remain in force for as long as the service relating to the processing of personal data is provided. During this period, the Clauses may not be terminated unless other provisions governing the provision of the service relating to the processing of personal data are agreed between the Parties.

4. Where the provision of services relating to the processing of personal data ceases, and the personal data have been deleted or returned to the Data Controller in accordance with Clause 11.1 and Appendix C.4, these Clauses may be terminated by either Party upon written notice.

5. Signatures

   On behalf of the Data Controller

   Name
   Title
   Signature

   On behalf of the Data Processor

   Name
   Title
   Signature

14. Contact Persons of the Data Controller and the Data Processor

1. The Data Processor may be contacted via the contact person listed below or through communication with the persons who are ordinarily involved in the contractual relationship between the Data Controller and the Data Processor.

2. The Parties may contact each other via the contact persons listed below.

3. The Parties shall be obliged to continuously inform each other of any changes relating to the contact persons. If it is not possible for the Data Processor to reach the Data Controller through the stated contact person, the Data Controller hereby permits the Data Processor to contact another person who is ordinarily involved in the contractual relationship between the Data Controller and the Data Processor.

   On behalf of the Data Controller

   Name
   Title
   E-mail

   On behalf of the Data Processor

Name	Privacy Team
Title	Privacy Team
E-mail	privacy.plandisc@visma.com

Appendix A Information on the Processing

A.1. Purpose of the Data Processor's Processing of Personal Data on Behalf of the Data Controller

The processing of the Data Controller's personal data is carried out for the purpose of fulfilling the agreement entered into between the Data Processor and the Data Controller concerning the Data Processor's provision of its digital solution, which constitutes a virtual calendar solution.

A.2. Description of the Processing of Personal Data Carried Out by the Data Processor on Behalf of the Data Controller (Nature of the Processing)

As the owner and provider of the solution, the Data Processor processes personal data in connection with the general operation of the solution, including hosting, display, organisation, receipt, transmission, structuring, adaptation, implementation, searching, processing, storage, recovery, deletion, restriction, maintenance, development, logging, support, troubleshooting, and other IT services related to the Data Processor's solution(s) and/or service(s) provided to the Data Controller pursuant to the agreement entered into between the Parties.

A.3. Types of Personal Data Relating to Data Subjects

As a general rule, the Data Processor processes the categories of personal data set out below. However, through use of the solution, the Data Controller may entrust the Data Processor with the processing of any type of data and personal data, meaning that the Data Processor may potentially process all categories of personal data.

- **Ordinary personal data** (cf. Article 4(1) and Article 6 of the General Data Protection Regulation), such as name, telephone number, email address, and IP address.

A.4. Categories of Data Subjects

As a general rule, the Data Processor processes the categories of data subjects set out below. However, through use of the solution, the Data Controller may entrust the Data Processor with the processing of data and personal data relating to additional categories of data subjects.

Categories of data subjects:

- End users of the Customer

A.5. Duration of the Processing

The Data Processor's processing of personal data on behalf of the Data Controller may commence upon the entry into force of these Clauses. The processing is not time-limited and shall continue until these Clauses are terminated.

Appendix B Sub-processors

B.1. Approved Sub-processors

As of the entry into force of these Clauses, the Data Controller has approved the use of the following sub-processors:

NAME	COMPANY REGISTRATION NO.	ADDRESS AND COUNTRY / LOCATION OF PROCESSING	DESCRIPTION OF PROCESSING	TRANSFER MECHANISM (IF APPLICABLE)
Amazon AWS	LU26888617	38 avenue John F. Kennedy, L-1855 Luxembourg	Amazon Web Services (AWS) securely stores customer data via S3 Cloud Storage. Such processing is carried out in accordance with AWS' standard sub-processing agreement.	AWS is certified under the EU–U.S. Data Privacy Framework, which constitutes the transfer mechanism for any transfers of personal data to third countries outside the EU/EEA.
Microsoft Azure	VAT: IE8256796U	South County Business Park, Leopardstown, Dublin 18, Ireland	Microsoft Azure is used as the hosting and infrastructure platform for the solution. Processing includes storage, processing, and operation of customer data in Microsoft's Swedish data centres in accordance with Microsoft's data processing agreement.	N/A
WebHosting A/S	25674138	Naverland 2, 2600 Glostrup, Denmark	WebHosting A/S sends and receives emails from the solution via SMTP services. Processing is carried out in accordance with their standard sub-processing agreement.	N/A
Ipregistry	VAT: FR13983391012	1 Chemin des Rosiers, 06800 Cagnes-sur-Mer, France	IPregistry is used to determine users' geographical locations (IP geolocation service). This functionality is primarily used to block access to the service from sanctioned countries subject to international embargoes. Processing is carried out in accordance with their standard sub-processing agreement.	N/A
Orca Security Ltd.	13410414	Frankfurt, Germany	Orca Security Ltd. is used to secure the cloud infrastructure by analysing networks, services, storage configurations, malware scanning, and updating operating systems used on virtual machines, managing access rights, and configuring multi-factor authentication (MFA) for users with infrastructure access. Processing is carried out in accordance with Visma's sub-processing agreement with Orca Security, which ensures, inter alia, that all data is processed within the EU/EEA.	N/A

Upon the entry into force of these Clauses, the Data Controller has approved the use of the above-mentioned sub-processors for the described processing activity. The Data Processor shall not, without the Data Controller's prior written approval, engage a sub-processor for a processing activity other than the described and agreed processing activity, nor engage a different sub-processor for such processing activity.

The Data Processor shall maintain an up-to-date list of sub-processors on the Data Processor's website, which shall constitute the applicable Appendix B from time to time. Copies of sub-processing agreements may be obtained via the website or upon written request to the Data Processor.

B.2. Notice Period for Objections to Changes of Sub-processors

The Data Processor's notification of any intended changes relating to the addition or replacement of sub-processors shall be made publicly available on the Data Processor's website no later than ten (10) days prior to the intended commencement of the use of, or change to, the sub-processor, to the extent reasonably practicable, cf. contractual provision Section 7, Clause 7.3.

Notwithstanding the above, the Data Controller acknowledges that there may be special circumstances in which a specific need arises for changes relating to the addition or replacement of sub-processors to take effect with shorter notice or with immediate effect. In such cases, the Data Processor shall notify the Data Controller of the change as soon as possible.

If the Data Controller objects to such changes, the Data Controller shall notify the Data Processor thereof prior to the notified effective date of the change. The Data Controller may only object where it has reasonable and substantiated grounds for doing so.

By raising an objection, the Data Controller acknowledges that the Data Processor may be prevented from delivering all or part of the agreed services. Any such inability to perform shall not constitute a breach by the Data Processor. The Data Processor shall remain entitled to payment for such services, notwithstanding that they cannot be delivered to the Data Controller.

.

Appendix C Instructions Regarding the Processing of Personal Data

C.1 Subject Matter of the Processing / Instructions

The Data Processor's processing of personal data on behalf of the Data Controller consists of the Data Processor performing the following activities:

operation, including hosting, display, organisation, receipt, transmission, structuring, adaptation, implementation, searching, processing, storage, recovery, deletion, restriction, maintenance, development, logging, support, troubleshooting, and other IT services related to the Data Processor's provision of its digital solution to the Data Controller pursuant to the agreement entered into between the Parties regarding the provision of the Data Processor's digital solution.

C.2 Security of Processing

The level of security shall reflect the scope and nature of the processing as set out in Appendix A, Sections A.1 and A.2, including the more detailed instructions set out in Appendix C, Section C.1.

Security Level:
Based on the above information regarding the processing, and taking into account the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the following security level shall be established:

Agreed Security Level
High

The Data Processor shall thereafter be entitled and obliged to determine which technical and organisational security measures are to be implemented in order to establish the necessary (and agreed) level of security.

The Data Processor shall support the Data Controller in its efforts to document the identified risks and how such risks have been reduced to an acceptable level, and shall implement the measures necessary to mitigate the identified risks.

Based on the established level of security, procedures for audits shall be implemented in accordance with Sections C.7 and C.8.

The Data Processor shall furthermore be entitled and obliged to determine which technical and organisational security measures are to be implemented in order to establish the necessary (and agreed) level of security.

However, the Data Processor shall, in all circumstances and as a minimum, implement the following measures as agreed with the Data Controller:

C.2.1 Requirements for Pseudonymisation and Encryption of Personal Data

Requirements for Pseudonymisation of Personal Data

The Data Processor shall apply pseudonymisation of personal data where the nature, scope, context, and purposes of the relevant processing, as well as the risks of varying likelihood and severity to the fundamental rights and freedoms of natural persons, so require.

Requirements for Encryption of Personal Data

The Data Processor shall apply encryption of personal data where the nature, scope, context, and purposes of the relevant processing, as well as the risks of varying likelihood and severity to the fundamental rights and freedoms of natural persons, so require.

The Data Processor shall ensure that the encryption used is properly configured and sufficient to safeguard the confidentiality and integrity of the personal data processed.

Upon instruction, encryption of personal data shall always be applied for any transmission of confidential and sensitive personal data via external communication networks.

C.2.2 Requirements Relating to the Ability to Ensure Ongoing Confidentiality, Integrity, Availability, and Resilience of Processing Systems and Services

1. The Data Processor shall carry out a risk assessment at least once annually for each of the processing systems and services in which the Data Controller's personal data are processed. Based on the results of such risk assessments, the Data Processor shall loyally and professionally implement mitigating measures.
2. The Data Processor shall continuously implement technical and organisational mitigating measures where this proves necessary.
3. The same requirements shall apply to the Data Controller where mitigating measures can only be implemented by the Data Controller itself through its use of the solution.

The Data Processor shall further ensure that:

1. access to the personal data covered by the agreement is restricted to persons who have a legitimate business purpose;
2. technical and/or organisational measures are in place to ensure that only such authorised persons have access; such authorisation shall also apply to persons performing consultancy services or necessary audit, operational, or system-technical tasks;
3. regular checks are carried out to verify that users have been granted only the access rights and authorisations appropriate to their role;
4. employees and any collaborators are at all times aware of, and have received sufficient training and instruction regarding, the purposes of the processing, relevant policies, procedures, workflows, and their duty of confidentiality.
5. The Data Controller shall be subject to the same requirements with respect to its own organisation.

C.2.3 Requirements Relating to the Ability to Restore the Availability of and Access to Personal Data in a Timely Manner in the Event of a Physical or Technical Incident

The Data Processor shall ensure that:

1. up-to-date and effective contingency plans and procedures are in place to ensure the restoration of personal data and access thereto within a reasonable timeframe in the event of operational disruptions;
2. regular backups are performed of personal data covered by the agreement;
3. the effectiveness of technical and organisational security measures for ensuring processing security is regularly tested and evaluated through the conduct of IT contingency and disaster recovery exercises.

C.2.4 Requirements Relating to Procedures for Regular Testing, Assessment, and Evaluation of the Effectiveness of Technical and Organisational Security Measures

Procedures shall be in place to ensure regular testing, assessment, and evaluation of the effectiveness of the technical and organisational security measures implemented to ensure the security of processing.

The Data Processor shall at all times maintain up-to-date procedures for:

1. regular monitoring, assessment, adaptation, and improvement of the effectiveness of technical and organisational security measures required under applicable legislation, case law, decisions, recommendations, and guidelines issued by the supervisory authority, as well as under this Data Processing Agreement;
2. verification that security measures are effectively complied with in relation to the prevailing risk to the rights and freedoms of data subjects;
3. review and control of user access for employees and other authorised persons;
4. verification that backups are readable, write-protected, of appropriate scope, and capable of being restored;
5. verification of proper encryption, including secure storage of encryption keys;
6. verification that security logs are sufficient and relevant;
7. verification that the level of physical security is aligned with the current threat landscape.
8. The Data Processor shall maintain formal change management procedures to ensure that any changes are duly authorised, tested, and approved prior to implementation.
9. For critical security updates, the Data Processor shall maintain procedures ensuring that such updates can be implemented without undue delay.
10. Extraordinary controls shall be conducted in connection with major changes to system configurations and following any personal data breach.

C.2.5 Requirements Relating to Access to Personal Data via the Internet

Where systems containing personal data are accessed via the internet, user authentication shall be based on multi-factor authentication. Access to personal data covered by these Clauses shall only be permitted via secure, encrypted connections.

C.2.6 Requirements Relating to the Protection of Personal Data During Transmission

Appropriate security measures shall be applied during the transmission of personal data. Such security measures shall comply with recognised and applicable industry standards for the processing of personal data.

The Data Processor shall ensure that personal data is encrypted during transmission. Encryption shall be kept up to date and shall comply with recognised and applicable industry standards at all times.

C.2.7 Requirements Relating to the Protection of Personal Data During Storage

During the storage of personal data, appropriate security measures shall be implemented, taking into account the nature of the personal data processed and the risks to the rights of data subjects. The Data Processor shall ensure that personal data is encrypted at rest and that access thereto is restricted to authorised persons through controlled access procedures.

C.2.8 Requirements Relating to Physical Security of Locations Where Personal Data Is Processed

The Data Processor shall ensure that appropriate security measures are in place to prevent unauthorised access to locations where the Data Controller's data is processed.

Such security measures shall be aligned with the current threat landscape and the sensitivity and volume of personal data processed on behalf of the Data Controller.

Processing shall take place from locations protected against damage caused by physical factors, including, but not limited to, fire, overheating, water damage, magnetism, utility failures, theft, and vandalism.

The Data Processor shall ensure that all equipment used in connection with the processing of personal data is subject to appropriate technical safeguards.

C.2.9 Requirements Relating to the Use of Home and Remote Workstations

Home and remote workstations shall be secured by technical controls ensuring that the processing of personal data complies with applicable law and the agreement entered into between the Parties.

Measures shall be in place to prevent unauthorised persons from accessing personal data processed at home or remote workstations, and employees shall be instructed on how to prevent such unauthorised access.

The Data Processor shall ensure that encrypted communication channels are used. Remote access shall be secured through a VPN solution or equivalent security technology, ensuring that only authorised persons may access personal data.

Authentication of persons accessing personal data shall be based on multi-factor authentication or equivalent security measures.

C.2.10 Requirements Relating to Logging

The Data Processor shall maintain logs of users' access to and use of the Solution to the extent necessary to document the processing and ensure compliance with applicable data protection legislation. As a minimum, logs shall contain relevant information sufficient to identify the nature and purpose of the use.

Automated logging shall be performed for all processing of personal data.

Logs shall, as a minimum, contain information regarding the time of access, user identity, type of use, and identification of the data subject to whom the accessed data related or the search criteria applied.

Log data shall be retained for a period proportionate to the purpose of the logging and shall thereafter be deleted, unless a longer retention period is established in accordance with the purpose of the logs, for example for investigative purposes. At the time of entry into this agreement, the applicable retention period is twelve (12) months; however, this period may be adjusted by the Data Processor in accordance with applicable security and operational requirements.

The Data Processor shall continuously verify that logs contain the information required under these Clauses. In the event of suspected misuse or a personal data breach, the Data Processor shall, at no cost, provide relevant log data, including timestamps, user identity, type of access or modification, and the functionality used, and ensure that such logs are presented in a clear and usable format.

C.3 Assistance to the Data Controller

To the extent possible, and within the scope and extent set out below, the Data Processor shall assist the Data Controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

Notification of the Data Controller of Data Subject Requests

The Data Processor shall, without undue delay after becoming aware thereof, notify the Data Controller in writing of any request addressed to the Data Processor or its sub-processors by a data subject regarding the exercise of the data subject's rights under applicable data protection law. The Data Processor shall not respond to such requests. Upon the Data Controller's request, the Data Processor shall assist the Data Controller in fulfilling its obligations with respect to data subjects' rights under applicable data protection law..

Assistance in the Event of a Personal Data Breach

The Data Processor's assistance in connection with the Data Controller's obligations under Articles 33 and 34 of the General Data Protection Regulation shall consist of providing the information set out in Clause 10.3 to the Data Controller within the timeframe specified in Clause 10.2. Upon request, the Data Processor shall further assist the Data Controller by making available any information necessary for the Data Controller to notify the personal data breach to the competent supervisory authority or to communicate the breach to the data subject.

Assistance in Risk Assessments and Data Protection Impact Assessments
The Data Processor shall assist the Data Controller by providing the information necessary for the Data Controller to carry out required risk assessments. Where the Data Controller assesses that the processing is likely to result in a high risk to the rights and freedoms of data subjects, the Data Processor shall, upon request, assist the Data Controller in fulfilling its obligations under Articles 35 and 36 of the General Data Protection Regulation, including by providing the information necessary to conduct a data protection impact assessment and to carry out prior consultation with the competent supervisory authority.

Ensuring Technical and Organisational Measures

The Data Processor shall ensure that its technical and organisational measures enable the Data Controller to comply with its obligations under Articles 33–36 of the General Data Protection Regulation, including through measures relating to incident management, asset management, logging, and similar measures set out in Appendix C.

C.4 Retention Period / Deletion Procedures

Personal data shall be stored by the Data Processor until the Data Controller requests deletion or return of the data.

Upon termination of the service or these Clauses relating to the processing of personal data, the Data Processor shall delete the personal data in accordance with Clause 11.1, unless the Data Controller has changed its original choice after signing these Clauses. Any such changes shall be documented and retained in writing, including electronically, together with these Clauses.

It is agreed that personal data which the Data Controller has independently assessed as subject to deletion shall be deleted, irrespective of any time limitation, and that the Data Processor shall support the Data Controller in deleting such personal data. In addition, the Data Processor shall be capable of deleting personal data upon specific request from the Data Controller.

C.5 Location of Processing

Processing of personal data covered by these Clauses shall not take place at locations other than those

specified in this Data Processing Agreement and the addresses of the engaged sub-processors, including further sub-processors, as set out in the applicable Appendix B, without the Data Controller's prior written approval.

C.6 Instructions Regarding Transfers of Personal Data to Third Countries

If the Data Controller has not provided documented instructions in these Clauses or subsequently regarding transfers of personal data to a third country, the Data Processor shall not be entitled to carry out such transfers under these Clauses, unless the transfer is made to an authorised sub-processor listed in Appendix B. Any transfer mechanism shall comply with Chapter V of the General Data Protection Regulation, and the applicable transfer mechanisms are set out in Appendix B.

Requests from Public Authorities for Disclosure of Personal Data

The Data Processor shall notify the Data Controller of any request received by the Data Processor or its sub-processors from a public authority in a third country for disclosure of personal data covered by these Clauses.

Where the Data Processor, directly or indirectly, receives a request to disclose personal data covered by these Clauses to a recipient located outside the EU/EEA, the Data Processor shall, to the extent permitted under Union law or Member State law, oppose such disclosure.

The Data Processor shall, where possible and in cooperation with the relevant sub-processor, exhaust all available remedies to challenge disclosure requests that are general in nature or not in compliance with Union law, including the General Data Protection Regulation, and applicable national legislation. To the extent possible, the Data Processor shall enable the Data Controller to participate in complaint or legal proceedings in order to protect its interests.

C.7 Procedures for Audits and Inspections Conducted by the Data Controller

Once annually and at its own expense, the Data Processor shall obtain an audit statement from an independent third party regarding the Data Processor's compliance with the General Data Protection Regulation, other applicable EU or Member State data protection law, and these Clauses.

The audit statement shall be an ISAE 3000 assurance report, providing a high level of assurance, prepared in accordance with the FSR standard, and covering the requirements set out in this Data Processing Agreement.

The Data Controller may deviate from the agreed audit model if it assesses that compliance can be demonstrated by other means. The Data Processor shall be entitled to separate remuneration where an alternative audit model is requested.

Audit statements and/or inspection reports shall be provided to the Data Controller without undue delay, unless already available on the Data Processor's website.
The Data Controller may challenge the scope and/or methodology of such reports and may request a new audit or inspection under different parameters and/or methodology against payment.

Based on audit results, the Data Controller may request the implementation of additional measures to ensure compliance with applicable data protection law and these Clauses.

The Data Controller, or an authorised representative, shall also be entitled to conduct inspections of the Data Processor's physical facilities where personal data are processed and receive the information necessary to verify compliance.

The Data Controller may disclose information obtained pursuant to this Appendix to the competent supervisory authority upon request.

C.8 Procedures for Audits and Inspections of Sub-processors

The Data Processor shall generally determine how audits of sub-processors' compliance are conducted, including the type and scope of audit statements and/or inspection reports, which shall reflect the nature of the processing carried out by the sub-processor.

Audit results shall be made available at least once annually via the audit model selected under Section C.7. The Data Controller may challenge the audit scope or methodology and request a new audit against payment. Based on audit results, the Data Controller may request additional measures to ensure compliance, against payment.

The Data Processor, or its representative, may conduct inspections, including physical inspections, of sub-processors' facilities and systems where necessary.
The Data Controller may also request such inspections where deemed necessary, subject to remuneration to the Data Processor.

Documentation of such inspections shall be included in the audit model selected under Appendix C, Section C.7. The Data Controller may challenge the inspection framework and request a new inspection under different parameters and/or methodology against payment.

Where necessary, the Data Controller may, upon reasonable notice, initiate and participate in a physical inspection of a sub-processor. This shall be at the expense of both the Data Processor and the relevant sub-processor.

Such participation shall not affect the Data Processor's continued responsibility for the sub-processor's compliance with applicable data protection law. The Data Processor's liability shall be limited to data protection obligations and shall not extend to other aspects of the sub-processor's performance.

Any costs incurred by the Data Controller in connection with inspections shall be borne by the Data Controller. The Data Processor shall allocate the time and resources reasonably required to facilitate inspections. The Data Controller may disclose information obtained pursuant to this Appendix to the Danish Data Protection Agency upon request.

Appendix D Regulation of Other Matters Between the Parties

D.1 Liability and Breach

The Parties' agreement on liability, including limitation of liability, is set out in the agreement entered into between the Data Processor and the Data Controller regarding the Data Processor's provision of the digital solution to the Data Controller, provided that such agreement does not directly or indirectly conflict with these Clauses or diminish the fundamental rights and freedoms of data subjects as set out in the General Data Protection Regulation.

D.2 Deletion and Return of Data

The Parties have agreed that the Data Controller shall instruct the Data Processor regarding the deletion and return of personal data upon termination of these Clauses.

No later than 30 days after the processing of personal data has ceased, the Data Controller shall notify the Data Processor whether all personal data are to be deleted or returned to the Data Controller. Where personal data are to be returned to the Data Controller, the Data Processor shall also delete any remaining copies. The Data Processor shall ensure that any sub-processors likewise comply with the Data Controller's instructions.

If the Data Processor has not received such notification from the Data Controller within **30 days** after the processing of personal data has ceased, the Data Processor shall send a reminder to the Data Controller. If the Data Controller thereafter fails to notify the Data Processor whether the personal data are to be deleted or returned, the Data Processor shall be entitled, without further notice, to delete the personal data.

The Data Processor shall be entitled to remuneration for its processing activities up to the time when the Data Controller notifies the Data Processor whether the personal data are to be deleted or returned.

D.3 Fees

Unless otherwise expressly agreed in this Data Processing Agreement, the Data Processor shall perform its obligations without separate remuneration. If the Data Controller's requests result in additional work exceeding a reasonable time expenditure (5 hours), the Data Processor may charge for the time spent, subject to further agreement between the Parties.

By way of example, where the Data Processor has, without undue delay, notified the Data Controller of a personal data breach in accordance with Clause 10, and such breach is attributable solely to circumstances on the part of the Data Controller, the Data Processor shall be entitled to separate remuneration for the time spent on such notification.

Appendix E **The Data Processing Chain**

The Data Processor undertakes to maintain an up-to-date and accessible overview of all sub-processors. The Data Controller may at any time review such overview.

The Data Processor further undertakes to comply with the forthcoming harmonisation of a common European **"standardised format"** for the specification of data processing chains and shall implement such format without undue delay upon its adoption and publication at EU level.

Data Processor:	Visma Plandisc A/S	Company Registration Number:	37204854
System Name:	**Plandisc**		

.