plandisc

Data Processing Agreement

Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

[NAME]
CVR [CVR-NR]
[ADDRESS]
[POSTAL CODE AND CITY]
[COUNTRY]

(the data controller)

and

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

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

Contents

1. Preamble

1. These Contractual Clauses (the Clauses) determine the rights and obligations of the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 (General Data Protection Regulation).

3. In the context of the license provision to Plandisc, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

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

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.

8. Appendix C contains the data controller's instructions with regards to the data processor's processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (GDPR) or any other legislation.

2. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purpose(s) and means of the processing of personal data.

3. The data controller is responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, along with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions

4. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no
   longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the above-mentioned confidentiality.

5. Security of processing

1. Article 32 GDPR stipulates that, taking into account the current technical level, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner

d. a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organizational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

4. If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor, the data controller shall specify these additional measures to be implemented in Appendix C.

6. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfillment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of 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 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorized by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the European Union or Member State law shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR. The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller’s request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfill his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfillment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. Transfer of data to third countries or international organizations

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

2. In case transfers to third countries or international organizations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

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

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

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

4. The data controller’s instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot constitute basis for transfer of personal data as referred to in Chapter V GDPR.

8. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfillment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.4., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring
compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Datatilsynet, 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 without undue delay communicate the personal data breach to the data subject, when 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 to carry out an assessment, prior to the processing, 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, Datatilsynet, 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 Data Processor's obligations under the Agreement shall not give rise to a claim for separate payment to the Data Processor for time spent, unless the time spent exceeds five (5) hours.

4. The parties shall define in Appendix C the appropriate technical and organizational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

9. Assistance to the data controller

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

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, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

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

    b. the likely consequences of the personal data breach;

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

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless the data controller instructs otherwise or Union or Member State law requires storage of the personal data.

11. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12. The parties' agreement on other terms

1. The parties may agree to other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

12. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the data controller

Name	[insert name]
Position	[insert position]
Date	[insert date]
Signature	[insert signature]

On behalf of the data processor

Name	Morten Olesen
Position	Head of Sales

14. Data controller and data processor contacts/contact points

1. The data processor can be contacted via the contact person below or by contacting persons who are usually communicated with in the contractual relationship between the data controller and the data processor.

2. The parties may contact each other using the following contacts/contact points:

3. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.
   If it is not possible for the data processor to reach the data controller through the contact person provided, the data controller allows the data processor to contact another person who is normally communicated with in the contractual relationship.

Name	Dennis Flæng Jørgensen
Position	Head of IT
Email	privacy@plandisc.com

Name	Morten Olesen
Position	Head of Sales
Email	morten.olesen@visma.com

Appendix A - Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is

The processing of the data controller's personal data takes place for the purpose of fulfilling the agreement entered into between the data processor and the data controller regarding the data processor's delivery of the data processor's digital solution.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing)

As the owner and provider of the solution, the data processor processes general operations, including hosting, displaying, organizing, receiving, forwarding, structuring, customizing, implementing, searching, processing, storing, restoring, deleting, restricting, maintaining, developing, logging, supporting, troubleshooting and other IT services associated with the data processor's solution(s) and/or service(s) for the data controller in accordance with the agreement between the parties.

A.3. The processing includes the following types of personal data about data subjects

The data processor generally processes the categories of personal data listed below. However, when using the solution, it is possible for the data controller to entrust the processing of all kinds of data and personal data to the data processor, which is why the data processor will potentially be able to process all categories of personal data.
General personal data (cf. Article 4(1) and Article 6 of the General Data Protection Regulation):
General personal data such as name, phone number, email, IP address

A.4. Processing includes the following categories of data subject

The data processor initially processes the categories of data subjects listed below. However, when using the solution, it is possible for the data controller to entrust the processing of all kinds of data and personal data to the data processor, which is why the data processor will potentially be able to process personal data about several categories of data subjects.
Categories of data subjects:

- The customer's end users

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration

The processing is not time limited and lasts until the subscription agreement between the parties for the delivery of the data processor's tools to the data controller is terminated or canceled by one of the parties.

Appendix B - Sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorizes the engagement of the following sub-processors:

Name	Org no.	Location	Description of processing	Transfer basis (if any)
Visma Data Center Visma Software International AS Karenslyst alle 56, Oslo, 0214, Norway	980 858 073	EU/EEA	Hosting	N/A
Safe Spring Safespring AB Rättarvägen 3, 169 68 Solna, Sweden	559075-0245	EU/EEA	Backup	N/A
Webhosting.dk WebHosting A/S Naverland 2 DK-2600 Glostrup Danmark	25674138	EU/EEA	Email service	N/A

Appendix C - Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

General operations, including hosting, displaying, organizing, receiving, forwarding, structuring, adapting, implementing, searching, processing, storing, recovering, deleting, restricting, maintaining, developing, logging, supporting, troubleshooting, and other IT services related to the data processor's solution and/or service for the data controller in accordance with the agreement entered between the parties.

C.2. Security of processing

The level of security shall take into account the following:

The Data Processor's solutions and services generally include the processing of personal data as covered by Article 6 of the General Data Protection Regulation and other confidential information. For this reason, the data processor has chosen to implement a generally high level of security to reflect the fact that such processing may take place. The data processor is then entitled and obliged to make decisions about the technical and organizational security measures to be implemented to establish the necessary (and agreed) security level.

However, the data processor must – in all circumstances and as a minimum – implement the following measures agreed with the data controller.

Information security
The data processor has implemented policies, controls, and processes that cover the information security areas described below:

Confidentiality: Ensure that unauthorized individuals cannot access data that can be misused to the detriment of the data processor's customers, business partners, and employees.
Integrity: Ensure that systems contain accurate and complete information.
Accessibility: Ensure that relevant information and systems are accessible and stable.

Instructions
There are written procedures that require that personal data may only be processed when there are instructions in place. An assessment is made on an ongoing basis – and at least once a year – of whether the procedures need to be updated.
The data processor only performs the processing of personal data that appears in the instructions from the data controller.

Physical and environmental security

The data processor shall maintain physical security measures to secure the premises used for the processing of personal data, including the storage of personal data covered by the Data Processing Agreement against unauthorized access and manipulation.
Must have appropriate technical measures to limit the risk of any unauthorized access to premises where personal data is processed. In addition, the data processor shall, where necessary, evaluate and improve the effectiveness of such measures.

Ensure that the level of physical security is at all times aligned with the current threat level as well as the sensitivity and volume of personal data covered by the data processing agreement.

Communication links and encryption

The data processor has appropriate technical measures to protect systems and networks, including protecting data during transmission and access via the internet, and to limit the risk of unauthorized access and/or installation of malicious code.

The data processor uses appropriate encryption technologies and other equivalent measures in accordance with legal requirements, and uses approved standards for encryption of classified information as well as good data processing practice.

To the extent required by applicable national and international legislation, and standards for encryption of classified information or good data processing practice, the data processor shall use encryption technologies and other equivalent measures.

Transmission of sensitive and confidential information over the internet is protected by encryption. Technological solutions for encryption are available and enabled. Firewalls only allow encrypted data traffic. Formalised procedures are in place to ensure that transmission of sensitive and confidential information over the internet is protected by strong encryption based on a recognised algorithm.

Firewall or similar technical measures

Access to systems and databases used for processing personal data is protected by firewalls. Administrative access must be available to maintain firewall configurations and rules.

Antivirus

For the systems and databases used for the processing of personal data, antivirus software is installed and regularly updated.

Back-up

The data processor must have internal contingency procedures that ensure the restoration of services without undue delay in the event of interruptions in operations under the main agreement. The data processor ensures daily backups.

Backups of configuration files and data must take place in an uninterrupted process so that relevant data can be restored. The backup copies shall be stored in such a way that they are not accidentally or illegally (e.g., by fire, flood, accident, theft or the like) destroyed, lost, impaired, disclosed to unauthorized persons, misused or otherwise processed in violation of the rules and regulations for the processing of personal data in force at any given time.

Backups must be stored physically separate from primary data and in a security-approved data center. Ensure that backups are stored in full length.

Use of home/remote workstations

If data processing is carried out from ad hoc and/or home offices, the data processor shall ensure that these comply with the security requirements in this Data Processing Agreement and its appendices and applicable legislation in general.

The data processor must, among other things, fulfill the following:
An encrypted connection is used between the ad hoc workplace and the Data Processor's/ Data Controller's network.
The data processor has internal instructions for its own employees regarding ad hoc and home offices.

In addition, the Data Processor must, if technically possible, use two-factor authentication.

Instruction of employees

The data processor ensures that employees are always aware of, and have sufficient training and instructions on, the purpose, policies, procedures, and confidentiality of the data processing.

There is an information security policy that has been reviewed and approved by the management within the last year. The information security policy has been communicated to relevant stakeholders, including the data processor's employees.

The information security policy generally meets the requirements for security measures and processing security in the data processing agreements that have been entered.
There are formalized procedures that ensure screening and verification of the data processor's employees in connection with employment.

Employees have signed a confidentiality agreement. Employees have been introduced to:

- The information security policy.
- Procedures regarding data processing, as well as other relevant information.

Procedures are in place to ensure that terminated employees' rights are deactivated or discontinued upon termination and that assets such as access cards, PCs, cell phones, etc. are confiscated. Terminated employees' rights are deactivated or discontinued and assets are retrieved.
Formalized procedures are in place to ensure that terminated employees are made aware of the maintenance of the confidentiality agreement and general duty of confidentiality. The employment contract contains guidelines stating that employees are subject to confidentiality obligations after terminated cooperation.

The data processor provides awareness training for employees covering general IT security and processing security in relation to personal data.

There is documentation that all employees who either have access to or process personal data have completed the awareness training offered.

Disposal of equipment

The data processor shall have formal processes in place to ensure the effective erasure of personal data prior to the disposal of electronic equipment.

Logging

1. Ensures logging in all environments where personal data is processed.
2. Activities performed by system administrators and others with special rights.
3. Changes to log setups, including disabling of logging.
4. Changes in system rights for users.
5. Ensures that the scope of the security log is defined based on a risk assessment performed by the data processor.
6. Ensures that there is enough space for the security logs to be stored for the period.
7. Ensures that ongoing random checks are carried out to make sure the security logs contain the expected information.
8. Balances the deletion deadlines of security logs with the ability to analyze cyberattacks, to support investigations, and to protect the rights and freedoms of citizens.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organizational measures:

Data subjects' rights, cf. section 9.1.

- The data processor shall assist in observing the rights of the data subjects by, among other things, being able to provide access to, delete, restrict, and correct information, and ensure that this also happens with the sub-processors.
- The data processor must assist in fulfilling the data subjects' rights without undue delay.
- The data processor must have a procedure in place for how to handle requests from a data subject regarding their rights.

Breaches and incidents, cf. section 9.2.

- Information to be sent:
- Facts about the detected breach (time, place, cause).
- When the breach started, when it was discovered, and when it was stopped.
- The nature of the personal data breach, including any breaches of confidentiality, integrity, and availability.
- The categories and approximate number of data subjects affected, if possible.
- The categories of personal data, if possible.
- Name and contact details of the point of contact where further information can be obtained.
- Description of the likely consequences of the breach.
- Description of measures taken, or proposed to be taken, to address the breach and its possible adverse effects.

C.4. Storage period/erasure procedures

Personal data is stored for the period of the agreement after which it is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses

C.5. Processing location

Processing of personal data covered by these terms may not, without the data controller's prior written approval, take place at locations other than those provided for in this data processing agreement and the addresses of the sub-processors used, as well as sub-processors in additional stages, as further described in the applicable Appendix B.

C.6. Instruction on the transfer of personal data to third countries

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer, unless such transfer is to one of the authorized sub-processors mentioned in Appendix B. Transfer basis is used in accordance with Chapter V of the Data Protection Regulation on transfers of personal data to third countries or international organizations. The specific transfer bases are set out in the applicable Appendix B.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall, within a period of 12 months, obtain at its own expense an ISAE 3000 audit opinion from an independent third party concerning the data processor's compliance with the Data Protection Regulation, data protection provisions in other EU or Member State law, and these Clauses.

The auditor's statement will be available to the data controller on the data processor's website.

The data controller may, against payment, challenge the framework and/or method of the declaration and may in such cases request a new declaration under a different framework and/or using a different method.

Based on the results of the statement, the data controller is entitled to request the implementation of additional measures in order to ensure compliance with the Data Protection Regulation, data protection provisions of other EU law, or the national law of the Member States and these Clauses.

In addition, the data controller or a representative of the data controller shall have the right, against payment, to carry out inspections, including physical inspections, of the premises from which the data processor processes personal data. Such inspections may be carried out whenever the data controller deems them necessary.

Any costs incurred by the data controller in connection with a physical inspection shall be covered by the data controller itself.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall annually at the data processor expense obtain a report concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

Upon request, documentation of such inspections shall be provided to the data controller for information purposes.

Appendix D - The parties' terms of agreement on other subjects

D.1. Liability and breaches

Any breach of the Clauses shall be governed and dealt with in accordance with the parties' agreement regarding the provision of the services.

In cases where the data processor has paid out amounts to data subjects in accordance with Article 82 of the Data Protection Regulation or Section 26 of the Danish Liability Act, the data processor shall have full recourse against the data controller for the amount paid out that exceeds the agreed limitation of liability in the parties'
agreement regarding the provision of the services.

The parties have thereby contractually derogated from Article 82(5) of the Data Protection Regulation and Section 26 of the Danish Liability Act.

Irrespective of Article 82(5) of the Data Protection Regulation, a party who has paid compensation to an injured party that does not correspond to full compensation may have recourse in accordance with the principle in Article 82(5).

In terms of other compensation for non-financial losses to data subjects, the principle of Article 82 shall also apply in regard to the internal final allocation of liability between the data processor and the data controller.

The parties may not assert recourse or claims for damages against the other party for fines or other penalties imposed pursuant to section 41 of the Data Protection Act and for fines accepted pursuant to section 42 of the Data Protection Act.

D.2. Consequences of any unlawful instructions from the data controller

The data controller is aware that the data processor is dependent on the data controller's instructions on the extent to which the data processor is entitled to use and process the personal data on behalf of the data controller. The data processor shall therefore not be liable for claims arising from the data processor's acts or omissions to the extent that these acts or omissions are a direct data processing activity carried out in accordance with the data controller's instructions, unless it can be established that the data processor was aware of the unlawfulness of the processing.

D.3 Use of sub-processor delivering on standard terms

Irrespective of contractual clause 7, it must be emphasized that if the data processor uses a sub-processor which provides services on its own terms that cannot be negotiated by the data processor, the sub-processor's terms apply to the processing activities entrusted to such sub-processor. Where processing is carried out on the terms of a sub-processor, this is indicated by the relevant sub-processor in the list of sub-processors. By these Clauses, the data controller accepts and instructs that such specific processing activities are carried out on the sub-processor's terms.

D.4 Deletion and return of information

It is agreed between the parties that the data controller shall instruct the data processor on the deletion and return of personal data in connection with the termination of the Clauses. The data controller shall, no later than 30 days after the processing of personal data has ceased, notify the data processor of whether all personal data shall be erased or returned to the data controller. In the event that personal data is to be returned to the data controller, the data processor shall delete any copies or backups. The data processor shall ensure that any sub-processors also comply with this notice from the data controller.

If the data processor has not received 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 does not subsequently notify the data processor of whether all personal data shall be deleted or returned to the data controller, the data processor is entitled to delete personal data without further notice.

The data processor is entitled to remuneration for its processing activities up to the point where the data controller notifies the data processor of whether all personal data shall be erased or returned to the data controller.