23 juni 2022

Standard Contractual Clauses

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

between

[NAME]
[CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]

(The data controller)

and

Vitec MV A/S
CVR-nr. 15 31 44 00
Edisonsvej 4
5000 Odense C

(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.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and 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 provision of Main contract of [DATE], 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 subject 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 authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the 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 (the GDPR) or other legislation.

3. 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[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

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

4. 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, in connection 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.

5. 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 abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, 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 organisational 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 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. 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 organisational 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.

   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 pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. 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 fulfilment 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 in writing the data controller 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 authorised 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 Clauses 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 organisational 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 fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment 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.

8. Transfer of data to third countries or international organisations

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

2. In case transfers to third countries or international organisations, 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 be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. 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 organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that 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 6.3., 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, 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 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, 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 define in Appendix C the appropriate technical and organisational 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.

10. Notification of personal data breach

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 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.

11. 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 Union or Member State law requires storage of the personal data.

12. 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.

13. The parties' agreement on other terms

1. The parties may agree 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.

14. 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	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

   On behalf of the data processor

Name	Tove Larsen
Position	Consultant
Telephone number	65 91 80 22
E-mail	Tove.Larsen@vitecsoftware.com
Signature	[SIGNATURE]

15. Data controller and data processor contacts/contact points

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

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	Carsten Peter Rasmussen
Position	CTO
Telephone	63 12 60 15
E-mail	CarstenPeter.Rasmussen@vitecsoftware.com

Appendix A Information about the processing

In the fulfilment of the Main Contract, the data processor shall provide the data controller with the following digital tools/software products:

- CD-ORD
- IntoWords

Data processor software products facilitate and simplify "text processing" for any given user. Text processing should be interpreted as these processes:

- Text comprehension: the product helps the user to understand written text using techniques such as reading aloud and highlighting text for the user
- Drafting text: user is supported with word suggestions and spelling assistance
- Speech to Text: Text is generated from speech. Conversion of speech to text is done by an API call to a third-party service.

A.1. Purpose of processing of personal data by the data processor on behalf of the data controller

Product services:
The aim of processing personal data in connection with the use of the data processor's products is to deliver the agreed service and to optimize the performance of the products, including creating the most effective learning, reading, and writing support for the user of the products/services, who thereby receives assistance in "reading and understanding a text", "writing a text" and "text speaking".

In order for the product to provide the above-mentioned support to the user, an account/user access must be created for each user. This log in/registration of the user helps the product to generate statistics for that user. This is done by the products/services recording the user's actions when in use, including how many word suggestions the user makes, text reading and converting images to text. However, the words and images are not recorded. It is therefore the function that is recorded, but not the content of the functions that is recorded.

End-user statistics:
When using the services, further processing of the user's personal data takes place for the purpose of creating end-user statistics. Statistics linked to the end user are based entirely on the number of uses of the services (including the number of word suggestions given and the number of readings of text). The products do not record the content or nature of text suggested/read. The end-user has the option to view his own statistics.

Statistics for product enhancements:
For the internal assessment of the products by the data processor, statistics are collected cumulatively for all users of the data processor's systems. These statistics are anonymized and completely dissociated from the end user. The data processor can deduct from the statistics how many word suggestions are given on a given day or time of day, but not in connection with the specific user.

Specific on Speaking - Speech to Text
Speech-to-text conversion is done using Microsoft Azure, offered by Microsoft. When the data processor receives the audio file with the user's speech, the data processor sends the audio file, together with other users' audio files,

to Microsoft in the Netherlands via an API for conversion to text. The sound file is terminated immediately after Microsoft has converted it.

No other information is sent with the audio file, and Microsoft has no way of linking the audio file to the user who recorded the audio file, and therefore no way of identifying that user. Consequently, while the sound file is in Microsoft's possession, it does not constitute personally identifiable information and therefore no processing of personal data is involved. Microsoft does not process the user's personal data at any time and is not a data sub-processor of the data processor.

A.2. The processing of personal data by the data processor on behalf of the data controller primarily relates to (nature of the processing)

The data processor's processing of personal data primarily consists in authentication of login information, including Unilogin information etc. on behalf of the data controller.

The data processor's products collect and record data about the user when creating a log-in/user account and when using the product/services to provide the agreed service.

For Business and Private customers, the name and e-mail of the user are registered to create user access. Data is stored as long as the user's access is active. Afterwards, data are anonymized and terminated.

In the case of Municipal customers, the data is pseudonymized. The name and email of the user are temporarily recorded during the login process. These data are stored as long as the user's access is active, i.e. the active user session, e.g. 30 min. The user's login-hash from the idP is stored permanently, but only as long as the user is associated with the data processor's login, or the corresponding contract is active. Statistical data is pseudonymized and associated only with the login-hash from the idP. This data is automatically terminated at the end of the contract.

When using the services of the data processor, the number of uses of the products' services by the user is recorded for the end-user statistics. This means that the number of word suggestions given and the number of readings of text etc. are recorded. The content or nature of text suggested or read to the user is not recorded.

Additional information about logging in
In order to use the services of the data processor, the creation of a valid login is necessary. Login can be done either with a so-called federated login via an identity provider (idP) or directly via the data processor's user management. In the latter case, the data processor acts as both login and idP.

In most cases, Municipal and Corporate clients use federated login and private users use the data processor's user management. Common to federated logins is that the data processor never extracts more data at login than is necessary to deliver the reading and writing assistive technology to clients. In most cases, only the user's internal hash value is stored. This means that users in the data processor's applications are pseudonymized for normal use and the data processor only knows the user's login. It is not possible for the data processor to trace data back to a specific person without considerable effort. For example, if a student at a given school, using the data processor's services, moves municipality, it would be impossible for the data processor to determine to which individual the pseudonymized login belonged without interfacing with data from UNI-C.

Common to all data that is not login/hash is that it is only retained for a short period by the data processor in connection with login.

A.3. The processing covers the following types of personal data relating to data subjects

Common to all types of clients is that the data processor only processes general personal data, cf. GDPR Art 6, and thus not personal data, cf. GDPR Art 9.

Municipal clients
All municipal clients in Denmark use UNI-C, in Norway Feide, in Sweden Skolfederation and in the Netherlands Entree. When logging in via these IDPs, certain personal data are made available to the data processor. However, this data is not used, and the data is not stored in the systems of the data processor. For some public clients Google idP or Microsoft idP is used and in these cases only tenant ID or root domain is exposed. This information is to be equated with the School Code.

Data about the user that is needed/provided to the data processor at login and use of the service constitutes the following:

Data	Stored / used by login
Role	Yes
Name	No
Address	No
Telephone number	No
E-mail	No
Business Identification	No
Municipality code	No
School code (institution number)	Yes
Class designation	Yes
Login / Hash	Yes

Corporate clients
In this case, login works in the same way as UNI-C, for instance, but it is completely up to the customer which data is included with login.

Data about the user that is needed/provided to the data processor at login constitutes the following:

Data	Stored / used by login
Role	Yes
Name	No
Address	No
Telephone number	No

E-mail	Yes
Business Identification	Yes
Municipality code	No
School code (institution number)	No
Class designation	No
Login / Hash	Yes

Private clients
The use and application of the services of the data processor by the customer requires the storage of personal data directly in the data processor's own login system.

Data on the user that is needed/provided to the data processor upon login constitutes the following:

Data	Stored/ used by login
Role	No
Name	Yes
Address	Yes
Telephone number	Yes
E-mail	Yes
Business Identification	No
Municipality code	No
School code (institution number)	No
Class designation	No
Login / Hash	Yes

A.4. The processing covers the following classes of data subjects

Staff assigned to data controllers	
Trainees/students assigned to data controllers	

Clients	
Children aged 6-17 years.	
Clients/private users	

A.5. The processing of personal data by the data processor on behalf of the data controller may start after the commencement of these Regulations. The duration of the processing shall be as follows kan påbegyndes efter disse Bestemmelsers ikrafttræden.

Processing of personal data by the data processor on behalf of the data controller shall start upon commencement of the main contract and shall continue until at the latest 30 days after termination of the main contract, where the data processor has deleted all personal data of the data controller prior to that date.

Data for Private clients is automatically deleted when the user account is closed by the user/client. All other data related to a user login is ephemeral and is only kept by the data processor as long as the user is logged in.

For termination of specific end users of Municipal and Business clients, termination will depend on notification by the data controller to the data processor, after which the termination will take place.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

Upon commencement of the Regulations, the data controller has authorized the use of the following sub-processors:

NAME	CVR	ADRESS	DESCRIPTION OF PROCESSING
Amazon Web Services		Dublin, Irland Greenhill Road, Tymon North, Dublin, Ireland	Server hosting
Vitec Software Group, Koncern IT		Göteborg, Sverige	Server hosting

Upon the commencement of the Regulations, the data controller has authorized the use of the above-mentioned sub-processors for the processing activity described. The data processor may not - without the written consent of the data controller - make use of a sub-processor for a processing operation other than that described and agreed to or make use of another sub-processor for that processing operation.

Appendix C Instruction pertaining to the use of personal data

C.1. Subject of processing/instruction

Processing of personal data by the data processor on behalf of the data controller is performed by the data processor as follows:

The data processor shall arrange for the data controller's users to create a user account/login so that the user may benefit from the services provided by the data processor's products/services, as described in Appendix A, including that the data processor records the data controller's/user's usage of the service/product for end user statistics.

C.2.Processing safety
The level of security must reflect:

The processing of personal data relates entirely to personal data of a general nature, cf. GDPR Art 6. Accordingly, no personal data are processed, cf. GDPR Art 9. However, the processing involves a large amount of personal data of users, including children under 16 years of age.

The data processor is then entitled and required to decide on the technical and organizational security measures to be implemented to establish the necessary (and agreed) level of security.

However, the data processor must - in any case and as a minimum - apply the following measures agreed with the data controller:

- Access to all data processor systems is secured with MFA and all data processor employees with access to operational environments have signed an enhanced privacy statement.
- The primary operating environment is AWS in Ireland, where data is hosted and where AWS's built-in CloudTrail is enabled. This means that all data processor employee logins and actions performed in operational environments are logged for 90 days. Audit logs are continuously monitored.
- The products use both "in transit" and "at rest" encryption. This means, among other things, that all connections to the backend are encrypted with TLS v1.3 "in transit". Encryption "at rest" depends on the media, but AES256 is most used.
- Encryption keys and certificates are issued via Let's Encrypt, AWS KMS or ACM.
- The data processor carries out continuous operational monitoring of the IT systems.
- Access to the data processor's network is secured, among other things, by using a firewall, VPN client and protected WiFi.

C.3 Aid to the data controller
The data processor shall, to the extent possible - within the scope and coverage set out below - assist the data controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organizational measures:

At the request of the data controller, the data processor may delete and extract all statistical data associated with the end user. For Business and Municipal clients, this aid requires that information from the IdP be provided by the data controller, as the data processor does not keep directly personally identifiable data for their users.

To delete data on behalf of the data controller, several technical steps are required depending on the type of user:

Municipal clients
Generally, a specific user cannot be identified in the data processor's system, as no directly personally identifiable information is stored on a user login. It is therefore necessary that, for example, UNI-C can be provided by the data controller of the specific user's login/hash, so that the data processor can extract it from the statistics database.

Business clients
The user can be identified by e-mail address, for example, and can be deleted/extracted based on this information.

Private clients
The user can be identified by. e.g. e-mail address, and data can be deleted/extracted based on this information.

C.4 Storage period/deletion routine

Personal data is kept until a user account is closed or for the period until the Main Contract ends and no later than 30 days from that date.
Private clients can delete their own user account.

C.5 Location for processing
Processing of the personal data covered by the Regulations may not be performed at locations other than the following without the prior written consent of the controller:

The processing of personal data covered by the Regulations is stored at the following locations by the following sub-processors hosting data on behalf of the data processor:

- AWS-datacenter
  Greenhill Road, Tymon North, Dublin, Ireland

- Vitec software Group, Göteborg, Sverige

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

If the data controller does not provide in these Regulations or subsequently a documented instruction regarding the transfer of personal data to a third country, the data processor is not authorized to make such transfers within the framework of these Regulations.

The data processor commits to use only sub-processors located
in the EU or secure third countries.

C.7 Procedures for data controller audits, including inspections, of the processing of personal data entrusted to the data processor

The data processor shall obtain annually, at its own expense, an audit opinion from an independent third party on the data processor's compliance with the GDPR, data protection regulations under other EU law or national law of the Member States and these Regulations.

It is agreed by the parties that the following types of audit opinions may be used in compliance with these Regulations:

ISAE 3000 or equivalent.

The audit report shall be transmitted without unnecessary delay to the data controller for information upon request. The statement shall also be published on the website of the data processor, www.vitec-mv.com

Based on the results of the declaration, the data controller is entitled to request the implementation of further measures to ensure compliance with the GDPR, data protection regulations of other EU law or Member States' national law and these Regulations.

In addition, the data controller or a representative of the data controller has access to carry out inspections, including physical inspections, of the premises from which the data processor undertakes the processing of personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out whenever the data controller finds it necessary.

The request for a physical inspection must be made with at least 30 days' notice. Any costs incurred by the data controller in connection with a physical inspection shall be covered by the data controller. The data processor shall be obliged to allow the time necessary for the data controller to conduct his inspection. The data controller shall be invoiced for the time and costs spent by the data processor in connection with such inspection, in accordance with the hourly rates set out in Appendix D.

C.8 Procedures for audits, including inspections, of processing of personal data entrusted to sub-processors

The processor shall regularly obtain from sub-processors, at its own expense, declarations or similar reports concerning the sub-processor's compliance with the GDPR, data protection regulations under other EU law or the national law of the Member States and these Regulations.

Appendix D The parties' terms of agreement on other subjects

Remuneration and costs

The data processor is entitled to payment, according to time spent, for services performed by the data processor within the scope of the Regulation and the data controller's request. The services may include, but are not limited to, amendments to the instruction, assistance with notification of personal data breaches, disclosure and erasure of data, assistance with audits, assistance with terminations, cooperation with supervisory authorities, and assistance with compliance with requests from data subjects.
Services may also include assistance with changes arising from new risk assessments.

The assistance of the data processor shall be settled as follows:

Consultant hourly rates: DKK 1.000 ex. VAT

Prices are adjusted in line with developments in the net price index.

Liability and limitations of liability

The liability of the parties for all cumulative claims under the Regulations is limited to the total payments under the Main Contract for the 12-month period ending immediately preceding the harmful act. If the Regulations have not been in in force for 12 months, the amount shall be calculated as the agreed payment of benefits under the Main Contract during the period the Regulations have been in force divided by the number of months the Regulations have been in force and then multiplied by 12.

Force Majeure

The data processor shall not be liable for circumstances that can generally be described as force majeure, including, but not limited to, war, riots, terrorism, insurrection, strikes, fire, natural disasters, currency restrictions, import or export restrictions, disruption of normal traffic, disruption or failure of energy supply, public data facilities and communication systems, viruses, and the occurrence of force majeure on the part of subcontractors. Force majeure may not be invoked for more than the number of working days during which the force majeure situation lasts.

Confidentiality

Information regarding the content of these Regulations, the underlying Main Contract, the business of the other Party, which either in connection with the transfer to the Party, or which by its nature or otherwise must clearly be regarded as confidential, shall be treated with the same care and discretion as the Party's own confidential information. Data, including personal data, shall always be considered confidential information.

However, the obligation of confidentiality shall not apply to information which is or becomes public accessible, without this being due to a breach of a Part's confidentiality obligation or information which is already in the possession of the receiving Party without a corresponding obligation of confidentiality; or

information independently developed by the receiving Party.

Dispute Resolution

The regulation of dispute resolution as set out in the Main Contract shall also apply to these Regulations as if the Regulations were an incorporated part of the Main Contract.