Standard Contractual Clauses (Data Processing Agreement)

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

between

[NAME]
[VAT Number]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the “data controller”)

and

Vitec MV A/S
CVR no. 15 31 44 00
CORTEX PARK VEST 3
5230 Odense M
Denmark

(the “data processor” or “Vitec”)

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 the services in accordance with the Main Contract dated [insert date] and any subsequent addenda entered into by the Parties, 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.

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

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

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 requires 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 thirty (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, where possible, 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 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 and Appendix B, B.1.

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. Considering 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, the Danish Data Protection Agency, 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, 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 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 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.

11. Erasure 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 GDPR 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, 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 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]
Phone number	[PHONENUMBER]
E-mail	[E-MAIL]
Signature	

On behalf of the data processor

Name	Tove Larsen
Position	Consultant
Phone number	65 91 80 22
E-mail	Tove.Larsen@vitecsoftware.com
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]
Phone number	[PHONENUMBER]
E-mail	[E-MAIL]

Vitec MV A/S

Name	Hans-Erik Schou
Position	CEO
Phone number	63 12 60 15
E-mail	support.mv@vitecsoftware.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 data processor, as part of fulfilling the Main Contract, provides the following digital aids/software products to the data controller:

- CD-ORD
- IntoWords

The data processor's software products support and simplify "text processing" for a given user. Text processing should be understood as these processes:

CD-ORD:

- Text comprehension: The product assists the user in understanding written text through techniques such as text-to-speech and text highlighting for the user.
- Text composition: The user is supported with word suggestions and spell-check.

IntoWords:

- Text comprehension: The product assists the user in understanding written text using techniques such as reading aloud and marking text for the user.
- Text composition: The user is supported with word suggestions, spell check, and speech-to-text.
- Speech-to-text: Text is generated based on speech input. Conversion of speech to text occurs through API calls to a third-party service. The conversion of speech to text takes place as follows: the end user transmits speech to the data processor's service, after which the data processor's service transmits it to MS Azure for processing. MS Azure then sends a response back to the data processor's service. Subsequently, the data processor's service transmits the text back to the end user. Audio files are automatically deleted both at the data processor and MS Azure after the described processing is completed.
- Translation: Translation is generated by having the end user transmit text to the data handler's service, after which the data handler's service transmits it to Amazon for processing. Amazon then sends a response back to the data handler's service. Afterward, the data handler's service transmits the translation back to the end user. Text is automatically deleted both at the data handler and Amazon after the described processing is completed.

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):

The data processor's processing of personal data primarily involves, on behalf of the data controller, authenticating login information, including Unilogin information, etc., in order to provide the services outlined in A.1.

The data processor's products collect and record user data during the creation of login/user accounts and during the use of the product/services to deliver the agreed-upon service.

For Municipality customers, data is pseudonymized. The user's login hash from idP is stored permanently, but only as long as the underlying contract is active.

For Business customers, the customer's administrator creates user logins themselves.

Further regarding logins
To use the data processor's services, the creation of a valid login is required. Login can be done either through a so-called federated login via an identity provider (idP) or directly through the data processor's user management. In the latter case, the data processor functions as both the login and idP.

Most often, Municipality and Business customers use federated logins. Common to federated logins is that the data processor never retrieves more data during login than is necessary to provide the product to the customers. Only the user's internal hash value is stored. This means that users in the data processor's programs are pseudonymized during regular use, and the data processor only knows the user's login. It is not possible for the data processor to attribute data to a specific person without significant effort. For example, if a student at a given school, a user of the data processor's services, moves to a different municipality, it would be impossible for the data processor to determine which person the pseudonymized login belonged to without matching it with data from UNI-C.

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

Municipality Customers
All municipality customers in Denmark use UNI-C, in Norway, Feide is used, in Sweden, Skolfederation is used, and in Holland, Entree is used. For some public customers, Google idP or Microsoft idP is used, and in these cases, only the tenant ID or root domain is provided. This information is equivalent to School Code.

The data about the user made available to the data processor during login and service usage includes the following:

- Role (e.g., student or teacher)
- School code (institutional number)
- Class designation
- Login/hash
- Text comprehension: In the context of delivering services, the text-to-speech of the marked text may contain personal data from the text itself.
- Text composition: In the context of delivering services, the text will contain the information, including personal data, that the end user may write.
- Speech-to-text: In the context of delivering services, the audio file itself will contain the end user's voice, including the information the end user may speak and

information that can possibly be inferred from the voice/sound, such as gender and language.
- Translation: In the context of delivering services, the translated text will contain the information, including personal data, that the end user may write.

The data processor does not, generally, process special categories of personal data (sensitive personal data, as per Article 9) under these Clauses, unless the data controller has provided instructions to do so in the Main Contract, other separately entered into agreements, or addenda.

If the data controller or the data controller's end users transmit or otherwise make special categories of personal data available to or through the data processor, including its sub-processors, the extent of which is determined and controlled by the data controller, it is considered that the data controller has given an instruction to the data processor to process these special categories of personal data in accordance with these Clauses.

It should be noted that the information transmitted by the end user in connection with the delivery of services is only retained for 7 (seven) days for the purpose of providing the service and any potential support. After this period, this information is deleted.

For Business Customers
In this case, login works in the same way as, for example, with UNI-C, but it is entirely up to the customer which data accompanies the login.

The data about the user made available to the data processor during login includes the following:

- Role (e.g., employee or administrator)
- Login/hash
- Text comprehension: In the context of delivering services, the text-to-speech of the marked text may contain personal data from the text itself.
- Text composition: In the context of delivering services, the text will contain the information, including personal data, that the end user may write.
- Speech-to-text: In the context of delivering services, the audio file itself will contain the end user's voice, including the information the end user may speak and information that can possibly be inferred from the voice/sound, such as gender and language.
- Translation: In the context of delivering services, the translated text will contain the information, including personal data, that the end user may write.

The data processor does not, generally, process special categories of personal data (sensitive personal data, as per Article 9) under these Clauses, unless the data controller has provided instructions to do so in the Main Contract, other separately entered into agreements, or addenda.

If the data controller or the data controller's end users transmit or otherwise make special categories of personal data available to or through the data processor, including its sub-processors, the extent of which is determined and controlled by the data controller, it is considered that the data controller has given an instruction to the data processor to process these special categories of personal data in accordance with these Clauses.

It should be noted that the information transmitted by the end user in connection with the delivery of services is only retained for 7 (seven) days for the purpose of providing the service and any potential support. After this period, this information is deleted.

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

Employees affiliated with the data controller	
Students affiliated with the data controller who are over 18 years old	
Students affiliated with the data controller who are under 18 years old	
Other data subjects, such as citizens	

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 data processor's processing of personal data on behalf of the data controller commences upon the effective date of the Main Contract and continues until no later than 30 days after the termination of the Main Contract, at which point the data processor has deleted all of the data controller's personal data.

For the deletion of specific end users among Municipality and Business customers, the deletion will depend on notification from the data controller to the data processor, after which the deletion will occur.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

The European Commission's standard contract clauses (model clauses) for the transfer of personal data to countries established outside the EU/EEA (also referred to as "Standard Contractual Clauses"), in accordance with the European Commission's implementing decision 2021/914 of June 4, 2021, on standard contract clauses for the transfer of personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council, will hereinafter be referred to as "Standard Contractual Clauses" or "SCC."

The EU-U.S. Data Privacy Framework, as per the European Commission's implementing decision of July 10, 2023, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, will hereinafter be referred to as "DPF."

At the commencement of these Clauses, the data controller has approved the use of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING	LEGAL BASIS OF TRANSFERS OF PERSONAL DATA
Amazon Web Services, South Dublin Data Center	N/A	Greenhills Road, Tymon North, Dublin, Ireland	Server hosting, Translation in the context of delivering online services	DPF List of covered entities by the DPF (is updated continuosly): https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000TOWQAA4&status=Active
Vitec Software Group, AB	N/A	Göteborg, Sweden	Server hosting	Not relevant
Microsoft Ireland Operations Limited, Microsoft Azure	N/A	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521	Speech-to-text, processing in the context of delivering online services	DPF List of covered entities by the DPF (is updated continuosly): https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the agreed purpose and processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

In accordance with Clause 7.3, the data processor notifies the data controller of any planned changes regarding the sub-processors specified in B.1. above, with a minimum of thirty (30) days' notice. This provides the data controller with the opportunity to object to such changes before implementation in connection with the execution of services on behalf of the data controller.

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:

The data processor ensures that data controllers/data controller's users can create user access/login for the purpose of enabling the user to utilize the services provided by the data processor's products/services, as described in Annex A.

C.2. Security of processing

The data processor shall implement all reasonable technical and organizational controls and measures, designed to safeguard the confidentiality, integrity and availability of the personal data it processes on behalf of the data controller. Personal data shall be properly classified, and appropriate security controls shall be implemented based on that classification.

In connection with the provision of services on behalf of the data controller, the data processor shall, at a minimum, apply the following security controls, which are based on the principles in the ISO 27001 standard and the controls in 'Control Objective B' regarding processing security in the ISAE 3000 statement:

C.2.1. Information Security Policy

C.2.1.1. The data processor, including its suppliers and employees, shall, at all times, comply with its internal Information Security Policy, which is aligned with the principles of the ISO27001 standard, which contains procedures designed to protect the security of the data controller's information and personal data while in the data processor's custody.

C.2.1.2. The data processor shall perform regular testing of its security policies, plans and controls, following a formal risk assessment process. The results of the above testing shall be communicated to the data processor's management, and findings directly affecting the processing of the data controller's personal data shall be remediated in a timely manner.

C.2.1.3. The data processor shall maintain and shall comply with the principles of the ISO27001 standard for the internal compliance program for information security policy and data protection.

C.2.2. Organization of Information Security

C.2.2.1. The data processor's information security organization must be structured in a way that allows for effective management and achievement of information security objectives.

Furthermore, the data processor shall:

a. retain suitably qualified personnel, with clearly defined roles and responsibilities, within its information security organization, to coordinate the implementation of security procedures for the data processor's organization.

b. determine requirements for sensitivity, protection and disclosure of information, and shall review such requirements annually.
c. segregate duties, roles and responsibilities, to prevent unauthorized use of the data processor's business critical information assets.

C.2.3. Human Resources

C.2.3.1. Background verification checks on employees that have access to personal data, shall be performed in accordance with relevant laws, regulations and ethical requirements and shall be performed for each individual at least upon initial hire, unless prohibited by law. The level of verification shall be appropriate according to the role of the employee, the sensitivity of the information to be accessed in the course of that person's role, and the risks that may arise from misuse of the information.

C.2.3.2. The data processor shall ensure that all personnel have signed confidentiality agreements as part of their employment contracts.

C.2.3.3. The data processor shall provide appropriate awareness training and access to information, so that the data processor's users understand their IT Security responsibilities, in relation to the data controller's information and personal data.

C.2.3.4. The data processor shall ensure that all necessary procedures are performed for the data processor's employees upon change of role, end of engagement, termination of employment, contract or agreement.

C.2.4. Asset Management

C.2.4.1. The data processor shall maintain procedures to identify, control and maintain the ownership and security classification of its key assets and the data controller's information and personal data held within the data processor's data center infrastructure.

C.2.4.2. The data processor shall create policies defining the acceptable use of information and assets and promulgate these to all appropriate users of its assets and information.

C.2.4.3. The data processor shall implement formal, documented system hardening procedures and baseline configurations. Unsupported software or hardware shall not be used.

C.2.5. Access Control

C.2.5.1. The data processor shall implement controls designed to safeguard access to the personal data processed on behalf of the data controller.

C.2.5.2. User access to data processor's systems and applications storing or allowing access to Personal data must be controlled by a secure login procedure.

C.2.5.3. Access to that personal data shall be granted to data processor's personnel on the basis of the need-to-know and least privilege principles, reflecting each individual's role and responsibilities.

C.2.5.4. The data processor shall monitor and restrict access to utilities capable of overriding system or application security controls. Administrator access rights to workstation endpoints shall be restricted.

C.2.5.5. A formal process shall be followed to timely revoke access to personal data when an individual is no longer required to have access to that information.

C.2.6. Cryptography

C.2.6.1. The data processor shall ensure that personal data processed on behalf of the data controller shall be protected at rest and in transit using strong encryption. Said encryption shall reflect generally accepted industry standards and shall be implemented in line with the data processor's encryption standard.

C.2.6.2. The data processor shall implement cryptographic key management procedures that include:

a. Generation of cryptographic keys with approved key lengths.
b. Secure distribution, activation and storage, recovery and replacement / update of cryptographic keys.
c. Immediate revocation (deactivation) of cryptographic keys upon compromise or change in user employment responsibility.
d. Recovery of cryptographic keys that are lost, corrupted or have expired.
e. Backup and archive of cryptographic keys and maintenance of cryptographic key history.
f. Allocation of defined cryptographic key activation and deactivation dates.
g. Restriction of cryptographic key access to authorised individuals.

C.2.6.3. The products utilize both encryption "in transit" and "at rest." This means, that all connections to the backend are encrypted with TLS v1.2/1.3 "in transit." Encryption "at rest" depends on the medium, but AES256 is most commonly used.

C.2.7. Physical and Environmental Security

C.2.7.1. The data processor shall implement physical security controls designed to protect the confidentiality, integrity and availability of the personal data processed on behalf of the data controller, at the data processors facilitates, client sites or third part locations. Those controls shall be periodically reviewed to ensure their effectiveness.

C.2.7.2. The data processor shall, at a minimum, apply the following physical security controls at its offices:

a. Physical access controls for buildings and critical areas;
b. Reception areas supervised by reception staff or security guard;
c. Logging of physical access or attempts thereof.

C.2.7.3. The primary operational environment used is AWS in Ireland, where data is hosted, and where AWS's built-in CloudTrail is activated. This means that all data processor employee logins and actions performed in operational environments are logged for 90 days. Audit logs are continuously monitored.

C.2.8. Operations Security

C.2.8.1. The data processor shall implement controls to detect and prevent malware, malicious code and the unauthorised execution of code. Controls shall be updated regularly with the latest technology available (e.g. deploying the latest signatures and definitions).

C.2.8.2. The data processor shall perform penetration testing for systems and applications that store or allow access to personal data.

C.2.8.3. The data processor shall implement a patch and vulnerability management process for systems and applications to identify, report and remediate vulnerabilities.

C.2.8.4. The data processor shall generate administrator and event logs for systems and applications that store or allow access to personal data.

C.2.8.5. The data processor shall review system logs periodically (minimum every 30 days) to identify system failures, faults, or potential security incidents affecting personal data. Corrective actions must be taken to resolve or address issues within any required timeframes.

C.2.9. Communications Security

C.2.9.1. The data processor shall deploy a secure Virtual Private Network (VPN) connection for its staff accessing its internal network remotely. Users shall use a two-factor authentication in order to enable the VPN connection.

C.2.9.2. The data processor shall deploy advanced firewalls to protect its network, including protection against malicious software and advanced intrusion techniques, as well as to segment its network to ensure resilience.

C.2.9.3. The data processor shall deploy solutions designed to monitor and log the activity on its network. The logs shall be continuously monitored to timely identify and remedy security incidents and shall be retained in accordance with the data processor’s formal policies and procedures.

C.2.9.4. The data processor shall synchronize system clocks on network servers to a universal time source (e.g. UTC) or network time protocol (NTP).

C.2.10. System Acquisition, Development & Maintenance

C.2.10.1. The data processor’s hardware, software, and service procurement process shall be documented and include identification and evaluation of information security risks.

C.2.10.2. The data processor shall implement formal, documented change control procedures to manage changes to information systems, supporting infrastructure, and facilities.

C.2.10.3. The data processor shall logically or physically separate environments for development, testing, and production. User access to program source code shall be restricted and tracked.

C.2.10.4. The data processor's secure system engineering and coding practices shall be established, documented and integrated within the system development life cycle (SDLC). Developers shall attend secure development training periodically.

C.2.10.5. The data processor's system and application changes shall undergo testing and meet defined acceptance criteria prior to implementation. Testing shall include relevant security controls.

C.2.10.6. The data processor's production data shall not be used within a non-production environment. If usage is unavoidable, data shall be masked (e.g. obfuscated, sanitised, de-identified, anonymised) or the non-production environment shall have security controls equivalent to those within the production environment.

C.2.10.7. The data processor's source code shall undergo automated static source code analysis and vulnerability remediation prior to implementation.

C.2.10.8. The data processor shall monitor outsourced system development activities, subject to third party supplier management controls.

C.2.11. Supplier Relationships

C.2.11.1. The data processor shall establish and maintain formal agreements with suppliers involved in the service delivery management of the data processor's information systems, incorporating where appropriate the necessary security controls, policies and service level agreements.

C.2.11.2. The data processor shall review its third parties' information security controls periodically and validate that these controls remain appropriate according to the risks represented by the third party's handling of personal data, taking into account any state-of-the-art technology and the costs of implementation.

C.2.11.3. The data processor shall restrict third party access to personal data. When access to data is necessary for performance of the contracted service, the data processor shall:

a. Provide the data controller a list of third parties with required access to personal data.
b. Permit access to personal data, only as necessary to perform the services that the third party has contractually agreed to deliver.
c. Record third party access to personal data, within system logs, subject to the data processor's controls for logging and monitoring.

C.2.12. Information Security Incident Management

C.2.12.1. The data processor shall prepare and maintain an incident response plan and program, containing procedures and directions to follow in the event of an incident related to the security of the data processor's computing infrastructure, documenting the necessary steps and channels of communication to be followed.

C.2.12.2. The data processor shall ensure that the directions incorporate appropriate procedures for notifying the data processor's clients, and other necessary stakeholders, promptly if any security incident is determined to have caused a security breach involving personal data.

C.2.13. Information security aspects of business continuity management

C.2.13.1. The data processor shall have a Business Continuity/Disaster Recovery plan in place that shall be used to recover the data processor's critical systems, applications and components in a timely manner in the event of a physical or technical incident.

C.2.13.2. The data processor shall test the above plans on a regular/annual basis and shall keep them up to date.

C.2.13.3 The data processor shall implement procedures to identify and validate backups required to support disaster recovery.

C.2.13.4 The data processor shall maintain appropriate backup retention to ensure disaster recovery and implement appropriate disposal procedures following retention requirements.

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 organisational measures:

Upon request from the data controller, the data processor can delete all data associated with the end user. For Business and Municipality customers, this assistance requires that information from the identity provider (idP) is provided by the data controller, as the data processor does not have direct personally identifiable data for these users.

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

Municipality Customers
In principle, a specific user cannot be identified in the data processor's system, as no directly personally identifiable information is stored on a user login. Therefore, it is necessary for the data controller to request UNI-C to identify the specific user, enabling the data processor to locate and delete data.

Business Customers
The user can be identified using, for example, an email address and can be deleted/located based on this information.

C.4. Storage period/erasure procedures

Personal data is retained until a user account is closed or during the period until the Main Contract terminates, but no later than 30 days thereafter.

Please note that information generated in connection with the delivery of services is deleted after 7 (seven) days, as outlined in section A.3.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

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

Additionally, processing can take place at any time at locations where the data processor's employees have home offices or similar arrangements.

The processing of the personal data covered by these provisions is stored at the following locations by the following sub-processors who host data on behalf of the data processor:

NAME	ADDRESS	LOCATION OF DATA CENTER	GEOGRAPHICAL LOCATION OF PARENT COMPANY
Amazon Web Services Inc., South Dublin Data Center ("AWS")	Greenhills Road, Tymon North, Dublin, Ireland	Personal data is stored in the AWS data center in Dublin.	USA
Vitec Software Group, Koncern IT	Göteborg, Sweden	Sweden	Sweden
Microsoft Ireland Operations Limited, Microsoft Azure ("Microsoft")	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521	Personal data is stored in Microsoft's data center located in Northern Europe	USA

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.

As part of the data processor's processing of personal data on behalf of the data controller, the data processor transfers personal data to USA.

The legal basis for the transfer to the USA is the EU-U.S. Data Privacy Framework (DPF), as per the European Commission's implementing adequacy decision of July 10, 2023, in accordance with Regulation (EU) 2016/679 of the European Parliament and the Council, as mentioned in Table B.1. At the commencement of these provisions, the European Commission has made an adequacy decision based on the EU-U.S. Data Privacy Framework (DPF), which constitutes a lawful transfer basis.

In the event that the DPF ceases to exist or is otherwise invalidated as a transfer basis, Standard Contractual Clauses will apply instead.

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 once a year at the data processor’s own expense obtain an auditor’s report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor’s report may be used in compliance with the Clauses:

ISAE 3000 report or any other report based on comparable or stricter standards.

Upon the data controller’s written request, the auditor’s report shall without undue delay be submitted to the data controller for information. The ISAE 3000 report is also published on the data processor's website, www.vitec-mv.com.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller’s representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and

related to the processing. Such an inspection shall be performed, when the data controller deems it required.

A request for a physical inspection must be made with at least 30 days' notice. Any expenses incurred by the data controller in connection with a physical inspection are the responsibility of the data controller themselves. The data processor is obligated to allocate the necessary time for the data controller to conduct their inspection. The data controller will be billed for the time and costs incurred by the data processor associated with such supervision.

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

The data processor shall once a year ensure that the sub-processor, at the sub-processor's expense obtain an auditor's report from an independent third party in respect of the security measures implemented by the sub-processor in compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses:

ISAE 3000, Soc 1 and Soc 2 type I or type II, or any other report based on comparable or stricter standards, or inspection based on the data processor's own requirements for external vendors' data processing and information security policies.
Where the sub-processor maintains an ISO 27001 or ISO 27701 certificate during the term of the Clauses, such certificate shall - possibly supplemented with management statements, etc. – be considered appropriate supervision.

Upon data controller's written request to the data processor, the data processor instruct the sub-processor to submit the auditor's report or the ISO 27001 or ISO 27701 certificate, as applicable, without undue delay to the data controller.

Procedures for audits, including inspections, concerning the processing of personal data entrusted to data processors and sub-processors, can be conducted at any time based on the form of supervision deemed appropriate in accordance with the Danish Data Protection Authority's "Guidance on Supervision of Data Processors."

Appendix D The parties' terms of agreement on other subjects

Responsibility and Liability

The parties' liability for all cumulative claims under the Clauses is limited to the total payments under the Main Contract for the 12-month period immediately preceding the harmful action.

Force Majeure

The data processor cannot be held liable for circumstances commonly referred to as force majeure, including but not limited to war, riots, terrorism, rebellion, strikes, fires, natural disasters, currency restrictions, import or export restrictions, disruption of public transportation, interruption or failure of energy supply, public data facilities, and communication systems, as well as the occurrence of force majeure with subcontractors. Force majeure can only be invoked for the number of working days that the force majeure situation lasts.

Confidentiality

Information related to the content of these Clauses, the underlying Main Contract, the other party's business, which is either designated as confidential information in connection with the transfer to the receiving party or which, by its nature or otherwise, can clearly be understood as confidential, must be treated confidentially and with at least the same care and discretion as the party's own confidential information. Data, including personal data, always constitutes confidential information.

However, the confidentiality obligation does not apply to information that is or becomes publicly available without a breach of a party's confidentiality obligation or information that is already in the possession of the receiving party without a corresponding confidentiality obligation or information that is independently developed by the receiving party.