Vendortell ApS

Data Processing Agreement

Version: 1.0

DATA PROCESSING AGREEMENT

Standard Contractual Clauses

Pursuant to Article 28③ of Regulation 2016/679 (the General Data Protection Regulation – "GDPR") for the purpose of the data processor's processing of personal data.

Between

Name:
CVR no:
Address:
ZIP code and city:
Country:

(hereinafter 'the data controller')

and

Vendortell ApS
CVR no: 44417618
Address: Klamsagervej 35,
ZIP code and city: 8230 Åbyhøj,
Country: Denmark

(hereinafter '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.

2. Preamble

2.1. 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.

2.2. The Clauses have been designed to ensure the parties' compliance with Article 28③ 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).

2.3. In the context of the provision of the services offered by the data processor, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

2.6. 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.

2.7. 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.

2.8. 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.

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

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

2.11. These 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

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

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

3.3. The data controller shall be responsible, among others, 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

4.1. 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.

4.2. 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

5.1. 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.

5.2. 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

6.1. Article 32 of the 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.

6.2. According to Article 32 of the 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.

6.3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 of the 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 of the GDPR along with all other information

necessary for the data controller to comply with the data controller's obligation under Article 32 of the 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 of the GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1. The data processor shall meet the requirements specified in Article 28② and ④ of the GDPR in order to engage another processor (a sub-processor).

7.2. 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.

7.3. 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 4 weeks 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.

7.4. 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.

7.5. 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.

8. Transfer of data to third countries or international organisations

8.1. 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 of the GDPR.

8.2. 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.

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

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

8.3.2. transfer the processing of personal data to a sub-processor in a third country: or

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

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

8.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46②(c) and (d) of the GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V of the GDPR.

9. Assistance to the data controller

9.1. 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 of the 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

9.2. 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:

9.2.1. the data controller's obligation to without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority in the country where the controller is based unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

9.2.2. 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;

9.2.3. 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);

9.2.4. the data controller's obligation to consult the competent supervisory authority in the country where the controller is based, 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.

9.3. 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

10.1. 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.

10.2. The data processor's notification to the data controller shall, if possible, take place within 36 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 of the GDPR.

10.3. In accordance with Clause 9②①, 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 33③GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

10.3.1. 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;

10.3.2. the likely consequences of the personal data breach.

10.3.3. 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.

10.4. The parties shall in Appendix D define any additional 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

11.1. 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, cf. Appendix A.5, unless Union or Member State law requires the storage of the personal data.

11.2. The data controller can request that the data processor stores relevant data after the end of the service provision period according to the provisions specified in Appendix C.4.

12. Audit and inspection

12.1. 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.

12.2. 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.

12.3. 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

13.1. The parties may agree on 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

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

14.2. 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.

14.3. 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.

14.4. 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 Appendices A.5 and C.4., the Clauses may be terminated by written notice by either party.

15. Data controller and data processor contacts/contact points

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

With the data controller: The contact person provided by the data controller in the Vendortell platform.

With the data processor:

Name: Steen Steensen Blicher

Position: CEO

Telephone: +45 22851085

Email: steen@vendortell.com

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

16. Signature

On behalf of the data controller		On behalf of the data processor	
Name:	_____	Name:	Steen Steensen Blicher
Position:	_____	Position:	CEO & Co-founder
Signature:	_____	Signature:	Signed by: Steen Steensen Blicher AB66D3D17F2F41B...

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:

On a subscription basis, the data processor makes available the cloud-based services ("Services") of the Vendortell Platform to the data controller and its authorized users.

The Services can be accessed via the data processor's online web-platform. The data controller's use of the data processor's cloud-based Services is done by the data controller's self-service via the data processor's web-platform. The data controller's access requires authentication either through the data controller's own identity provider or through user accounts managed by the data processor, as further described in Appendix C.2.

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 provides a cloud-based platform for vendor, contract and spend management. The data processed through the platform consists principally of the data controller's commercial data, being contracts, vendor records, transaction data and spend data, which does not constitute personal data.

However, personal data may occur within this material incidentally, principally as the names, job titles and business contact details of employees and representatives of the data controller and its vendors, where these appear in contracts, correspondence and vendor records, together with account and usage data for the data controller's authorised users.

The data processor's processing of such personal data consists of storage, hosting, structuring, and making the data available to the data controller and its authorised users through the platform, together with deletion or return on the data controller's instruction.

The platform's analytical functions, including vendor risk assessment, spend analytics and incentive calculation, operate on commercial and transactional data. Personal data is not the object of these functions and is processed only to the extent it appears in the underlying documents and records.

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

The personal data processed by the data processor in connection with the data controller's use of the data processor's Services differ according to the category to which the data subject belongs:

The Data Controller, including contact persons on behalf of the Data Controller:

- Contact information of the data controller's representatives, including name, telephone, email, title, department, address
- Authentication credentials for platform access, including typical user information such as name, email, and any photo the user themselves have uploaded as part of completing their profile
- Usage data related to platform activities

Vendors and Customer Representatives:

- Name
- Business contact information (email, phone, address)
- Job title and department
- Communication records
- Contract signatories information

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

See the overview in section A.3.

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 continues as long as the Data Controller makes use of the Services provided by the Data Processor to which the Data Controller subscribes.

At the termination of the subscription agreement, the data controller shall decide between:

- Immediate data deletion after termination
- Exporting data in a machine-readable format prior to deletion

If the Data Controller has not notified its election on termination, the data will be retained for a 30-day period and deleted on its expiry.

If the data controller wishes to continue storing data with the data processor for a longer period, the data controller must reactivate or extend the subscription.

Appendix B - Sub-processors

B.1. Approved sub-processors

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

NAME	COMPANY REG. NO.	ADDRESS	DESCRIPTION OF PROCESSING
Hetzner Online GmbH ("Hetzner")	Registration Court Ansbach, HRB 6089 VAT ID No. DE 812871812	Industriestr. 25 91710 Gunzenhausen Germany	Hetzner is used for the operation of the Vendortell Platform, including compute and application hosting, database operation, block storage and object storage. Data in the platform, including any personal data, is therefore processed and stored by Hetzner as sub-processor. Data is encrypted in transit and at rest, and is processed and stored within the EU/EEA without transfer to third countries or international organisations. Personal data is processed under Hetzner's standard data processing agreement. A copy of the data processing agreement with Hetzner can be shared with the data controller on request.
Amazon Web Services EMEA SARL ("AWS")	R.C.S. Luxembourg B 186284 VAT ID No. LU 26888617	38 Avenue John F. Kennedy L-1855 Luxembourg Luxembourg	AWS is used for optical character recognition (OCR) of documents uploaded by the data controller, and for the operation of parts of the platform's supporting infrastructure, including storage of customer data. Documents, including any personal data contained in them, are therefore processed by AWS as sub-processor. It is noted that data is not used to train any models. Data is encrypted in transit and at rest, and is processed and stored within the EU/EEA. Eu-central-1 (Frankfurt) region is chosen as the primary selected data location.

NAME	COMPANY REG. NO.	ADDRESS	DESCRIPTION OF PROCESSING
			Under AWS's standard data processing addendum, AWS may access customer content from outside the EEA for the purpose of providing support and operating the services. Such access takes place on the basis of the EU standard contractual clauses incorporated into that addendum, together with the supplementary technical, organisational and contractual measures described therein. A copy of the data processing agreement with AWS can be shared with the data controller on request. The data processor is in the process of transferring the services currently provided by AWS to the other sub-processors listed in this Appendix B.1. Completion is expected by the end of 2026, after which AWS will no longer be used for any services involving the processing of customer data, and AWS will be removed from this Appendix.
Microsoft Ireland Operations Limited ("Microsoft")	Company ID 256796	One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland Invoiced by Microsoft Danmark ApS	The data controller makes use of the data processor's AI functionality (Azure OpenAI Services (API)) in the platform. Microsoft's large language models are used to analyse, extract and summarise contract and vendor information, and any personal data contained in the documentation submitted is therefore processed by Microsoft in that connection. The service is a stateless API service, and customer data is therefore not stored permanently by Microsoft as part of the data processor's use of the service, noting that prompt snippets may be retained for abuse-monitoring

NAME	COMPANY REG. NO.	ADDRESS	DESCRIPTION OF PROCESSING
			purposes. Customer data is not used to train Microsoft's models. The data processor uses a DataZone deployment model with Sweden Central as the primary selected data location. Azure OpenAI Service is furthermore configured as an EU Data Boundary Service (EU data zone), and processing may accordingly take place in any EU/EEA member state but never outside the EU/EEA. Microsoft's processing is governed by a data processing agreement, a copy of which can be shared with the data controller on request.
Mistral AI SAS ("Mistral")	R.C.S. Paris 952 418 325	15 rue des Halles 75001 Paris France	Mistral is used for optical character recognition of documents uploaded by the data controller. Any personal data contained in those documents is therefore processed by Mistral in that connection. Customer data is not retained by Mistral beyond the completion of the processing, and is not used to train Mistral's models. Data is processed within the EU/EEA without transfer to third countries or international organisations. A copy of the data processing agreement with Mistral can be shared with the data controller on request.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the 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 '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

See Clause 7.3.

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:

When the data controller uses the cloud-based Vendortell platform, the data processor processes such limited personal data included in the controller's data as uploaded or migrated to the Vendortell platform or otherwise shared with the data processor. All processing activities are performed to facilitate the vendor management, risk assessment, contract management, and the spend and incentive analytics functions of the platform.

The platform is designed with an API that enables integration with other systems. To the extent that the data controller chooses to enable such integrations, it is considered to be an instruction to Vendortell that there may be a transfer of information entered into the platform to such third-party systems in accordance with this agreement.

The data processor may anonymize information from customers and use it for statistical and analytical purposes, and otherwise only process information as per this agreement and as required by law, including in connection with a legal decision, regulatory requirements, or similar circumstances.

Please also refer to Vendortell's Terms of Service.

C.2. Security of processing

The level of security shall take into account that the processing primarily involves business contact information and related commercial data, with appropriate security measures implemented to protect the confidentiality and integrity of this information.

The data processor is obligated to make decisions about the technical and organisational security measures that are to be applied to create the necessary level of data security.

However, the data processor shall as a minimum implement the following measures:

Service and database location Vendortell's production and testing environments are physically separated.

- Production environment is located within the EU

- Testing environment is located within the EU

Data encryption Data is encrypted both during transport and at rest.

Database access controls Database access is strictly limited and controlled through:

Authentication security Where the data controller uses federated authentication, access to the platform can be authenticated through the data controller's own identity provider via OAuth or similar, and the data processor will consequently not create, store or manage passwords for such users. Password complexity, multi-factor authentication and account provisioning and deprovisioning are in those cases governed by the data controller's own policies and controls.

Where the data controller instead uses the data processors' account and user setup, this is managed by the data processor, and passwords are subject to complexity requirements and are stored only in hashed form. Multi-factor authentication is available and is enabled by default as part of this setup.

Backup policy

- Daily automated backups are performed
- Backup retention policies ensure data can be restored for at least 10 days

Physical security Vendortell's facilities implement appropriate physical security controls, including access card systems, and for production environment rely on the sub-processors', cf. appendix B, security measures.

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. and implement such measures which contribute to the data controller's ability to respond to requests for the exercise of the rights of data subjects.

The Vendortell platform, including its API, enables the data controller to search, access, correct, export and delete data relating to an individual data subject, and the data controller is expected to make use of this functionality in the first instance to fulfill any request received from data subjects. Where a request cannot be fulfilled in this way, the data processor shall upon written request assist the data controller and respond within 10 working days.

C.4. Storage period/erasure procedures

Customer data, incl. any personal data, is stored in the Platform for as long as the data controller subscribes to the Services. The data controller may delete data at any time through the functionality made available in the Platform.

On termination of the subscription, the data controller elects between immediate deletion and retention for 30 days during which the data controller may export its data in a machine-readable format, cf. Appendix A.5. If the data controller makes no election, the data is retained for the 30-day period and deleted on its expiry. A longer retention period may be agreed against payment, cf. Clause 11.2.

Deletion irrevocably removes the data from the production environment without undue delay. However, copies contained in backups are deleted in accordance with the backup rotation described in Appendix C.2. The data processor shall confirm deletion in writing on request.

C.5. Processing location

Processing of the personal data covered by the Clauses may not, without the data controller's prior general approval cf. C.1 and C.6 and prior notice to the data controller cf. Clause 7.3, take place at locations other than the data processor's premises and the locations outlined in Appendix B.1.

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

The sub-processors engaged by the data processor are established in the EU/EEA, and personal data is processed within the EU/EEA as described for each sub-processor in Appendix B.1.

The data processor may not transfer personal data to a third country or an international organisation, or permit access to personal data from outside the EEA, except as set out in this Appendix C.6 or on the data controller's documented instruction.

As described in the AWS entry in Appendix B.1, AWS may under its standard data processing addendum access customer content from outside the EEA for the purpose of providing support and operating its services. The data controller instructs and authorises the data processor to permit such access for the purpose of the data processor's provision of the Services to which the data controller subscribes. Such access takes place on the basis of the EU Commission's standard contractual clauses incorporated into AWS's data

processing addendum, together with the supplementary technical, organisational and contractual measures described therein.

The data processor is responsible for ensuring that any transfer of personal data to a third country is carried out in accordance with Chapter V of the GDPR. If a transfer tool relied upon ceases to provide an adequate basis for a transfer, or a sub-processor is no longer able to comply with it, the data processor shall suspend the transfer concerned and inform the data controller without undue delay.

As set out in Appendix B.1, the data processor is transferring the services currently provided by AWS to the other sub-processors listed in that appendix. On completion, all processing of personal data under the Clauses will take place within the EU/EEA.

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, upon request, make available the documentation necessary for the data controller to assess the data processor's compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Provisions. This includes responding to reasonable security questionnaires and providing the data processor's security documentation, together with any assurance reports obtained from sub-processors. Requests shall be responded to within 30 working days.

If the documentation provided does not sufficiently resolve the data controller's questions, the data controller may, once annually and on no less than 30 days' written notice, conduct an inspection at the data processor's premises. Inspections shall take place during normal business hours, with minimum disruption to the data processor's operations, and subject to confidentiality, including in respect of the data processor's other customers. The data controller shall bear its own costs in connection with an inspection. The data processor is obligated to allocate reasonable resources (mainly time) necessary for the data controller to carry out its inspection.

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

The data processor conducts an annual compliance review of each sub-processor, based on the assurance reports, certifications and security

documentation made available by the sub-processor, including any ISO 27001 certifications, SOC 2 or ISAE 3000 reports available and equivalent documentation. Where a sub-processor makes on-site inspection available, the data processor may conduct such inspection where the data processor deems it necessary.

The documentation obtained shall be made available to the data controller on request. Where the data controller finds that this documentation does not sufficiently establish that the sub-processor's processing is carried out in accordance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Provisions, the data controller may at its own expense and risk request that further supervision be carried out, to the extent the sub-processor makes this possible. The data controller shall bear its own costs in connection with an inspection. The data processor is obligated to allocate the resources (mainly time) necessary for the data controller to carry out its inspection.

Appendix D – The Parties' agreement on other matters

The Parties have agreed on the following supplements for the Clauses:

For Clause 4.2 Notwithstanding Section 4.2, the data processor is not obliged actively to verify or investigate the legality of the data controller's instructions.

The data controller is aware that the data processor is dependent on the data controller's instructions on the extent to which the data processor is entitled to use and process the personal data on behalf of the data controller.

The data processor is therefore not liable for claims arising from the data processor's actions or omissions, to the extent that these actions or omissions are direct data processing activities carried out in accordance with the data controller's instructions.

For Clause 7 In its agreements with sub-processors, the data processor shall to the extent possible include the data controller as a third-party beneficiary in the event of the data processor's bankruptcy, so that the data controller can enter into the data processor's rights and assert them against the sub-processor. The data controller acknowledges that the sub-processors engaged by the data processor make their services available on standard terms which the data processor may not be able to negotiate, and that the data processor is accordingly not able to guarantee that such a provision can be obtained in each case.

For Clause 7.3 The data controller acknowledges that the data processor's Services are standardised, cloud-based subscription services made available to multiple customers and that the data processor is therefore not able to design the systems offered in such a way that each customer may require the data processor not to make use of specific sub-processors approved by the data processor.

Thus, the data controller acknowledges that if the data controller objects to the data processor's change or choice of new sub-processors and the data processor does not accommodate such an objection, the data controller's sole remedy is to terminate the subscription agreement with the data processor. The termination may take place with immediate effect, and neither party shall have any claim against each other in this connection.

For Clause 9.2 To the extent that the data controller wishes the data processor's assistance for the services described in Clauses 9.2③ and 9.2④, the data controller is obliged to remunerate the data processor for the time spent at the

hourly rates used by the data processor at the time, as shown on the data processor's website.

For Clause 13.1 The data processor's liability to the data controller is limited to what is set out in the subscription terms, including the terms of service, just as the other provisions of the subscription terms shall apply between the data controller and the data processor, except to the extent that they impair the fundamental rights and freedoms of the data subject under the General Data Protection Regulation.