Standard Contractual Clauses

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

between

“You” the Customer

(the data controller)

and

CAP TechCo ApS
VAT-No.: 44099578
Address: Dronningens Tværgade 26, 1302 Copenhagen K
Denmark

(the data processor)

each a ‘party’; together ‘the parties’

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

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 CAP Platform (a Venture Operating Platform), the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

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

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

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

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

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

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

3. The rights and obligations of the data controller

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

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

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

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

4. The data processor acts according to instructions

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

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

5. Confidentiality

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

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

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

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

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

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

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

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

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

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

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

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 work 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. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

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

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

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

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

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

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

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

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

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

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

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure (‘the right to be forgotten’)
   f. the right to restriction of processing

g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, 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 48 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 and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

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

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

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

13. The parties' agreement on other terms

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

14. Commencement and termination

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

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

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

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

5. Signature

   The Data Processing Agreement is automatically approved and signed by the data controller, when the data controller accepts Terms of Service.

   On behalf of You, the data controller, we collect

   Name
   Date
   Digital signature

   On behalf of the data processor

   Name
   Position
   Date

   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.

3. The contacts/contact points are automatically collected when You accept our Terms of Service.

   Data controller
   Name
   E-mail

   Data processor
   E-mail hey@cap.vc

5. 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:

- To process personal data related to the Cap VentureOS platform, which is a venture operating system that provides Deal Sourcing, Screening & Management, Portfolio & Investment Administration, Fund operations and Fund performance, Investor Management, a Chatbot and AI Assistant, and support services to the data controller.
- The data processor may produce a copy and use the data in anonymised form for the data processor's own statistical and analytical purposes to further develop the Platform.

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 shall analyse, structure, calculate, perform statistics and analytics, correct, store, search, perform reports, and delete the personal data.

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

Non-sensitive personal data:

- Employees of the data controller: User information and usage data, contact information (name, email, phone number), logging data, Financial information and ownership/investor information related to financial assets, corporate shares, and other securities), National ID (e.g. passport, driver's license, social security number)
- Business owners in portfolio: contact information (name, email, phone number), Financial information and ownership information related to financial assets, corporate shares, and other securities
- Employees of businesses in portfolio: contact information (name, email, phone number) employment information (title, experience, resume, certificates, accomplishments, employment agreement, salary, and other compensation)
- Investors of the data controller: contact information (name, email, phone number), Financial information and ownership/investor information related to financial assets, corporate shares, and other securities), National ID (e.g. passport, driver's license, social security number)
- Other personal data, the data controller may upload to the CAP Platform.

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

- Employees of the data controller
- Business owners in portfolio
- Employees of businesses in portfolio
- Investors of the data controller

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

The processing is not limited in time. These clauses remain in effect until there is no longer an active agreement between the data controller and the data processor regarding the data processor's processing of personal data and the data processor has irreversibly deleted all personal data processed on behalf of the data controller.

6. Appendix B Authorised sub-processors

B.1. Approved sub-processors

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

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING	LIST OF SUB PROCESSORS
Cabal, Inc.		316 Calle La Montana Moraga, CA 94556 United States	Email tool for collaboration and management	https://getcabal.com/privacy
Cloudflare, Inc.		101 Townsend St., San Francisco, CA, 94107. Data can be processed in other Cloudflare locations globally.	Provision of hosting services	https://www.cloudflare.com/en-gb/gdpr/subprocessors/
Clerk, Inc.		2261 Market Street STE 10607 San Francisco, CA 94114 USA	User authentication and management	https://clerk.com/legal/privacy
Google, LLC.		1600 Amphitheatre Parkway, Mountain View, CA 94043 Data can be processed in other Google locations globally.	Provision of hosting services	https://cloud.google.com/terms/subprocessors
AC PM, LLC (Postmark)		1 N Dearborn St, Suite 500, Chicago, IL 60602, USA	Communication with Authorized Users in connection with the provision of the Services and support	https://postmarkapp.com/eu-privacy#sub-processors
Fly.io, Inc.		2045 W Grand Ave, Ste B, Chicago, IL 60612, USA	Provision of hosting services	https://fly.io/legal/sub-processors/
Amazon Web Services, Inc.		410 Terry Ave N, Seattle, WA 98109 Data can be processed in other Amazon Web	Provision of hosting services	https://aws.amazon.com/compliance/sub-processors/archived/sub-processors_02082024/

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING	LIST OF SUB PROCESSORS
		Services locations globally.		
Slack Technologies, LLC.		500 Howard St, San Francisco, CA 94105 Using Amazon Web Services, Inc, processing potentially done globally.	Communication with Authorized Users in connection with the provision of the Services and support	https://slack.com/slack-subprocessors
Vercel, Inc.		440 N Barranca Ave, Suite 4133, Covina, CA 91723, USA	Provision of hosting services	https://security.vercel.com/?itemUid=e3fae2ca-94a9-416b-b577-5c90e382df57&source=click
Notion Labs, Inc.		2300 Harrison St, San Francisco, CA 94110 Using Amazon Web Services, Inc, processing potentially done globally.	Communication with Authorized Users in connection with the provision of the Services and support	https://www.notion.so/notion/Notion-s-List-of-Subprocessors-268fa5bcfa0f46b6bc29436b21676734?pvs=4
Linear Orbit, Inc.		340 S Lemon Ave, No. 4242, Walnut, CA 91789, USA	Project management and task tracking	https://linear.app/dpa
Transloadit-II GmbH		Waßmannsdorfer Chaussee 39 A, 12355 Berlin, Germany	Provision of file uploading and processing services	https://transloadit.com/legal/privacy/
Weaviate, B.V.		Prinsengracht 769a 1017 JZ Amsterdam	Provision of database services.	https://weaviate.io/subprocessors
Productlane GmbH		Albert-Roßhaupter-Str. 3b, 81369 Munic, Germany	Provision of customer feedback service.	https://productlane.com/privacy
Stripe, Inc.		354 Oyster Point Blvd, South San Francisco, CA 94080	Provision of payment system.	https://stripe.com/en-dk/legal/consumer#welcome

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 a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

7. 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:

To provide the CAP platform to the data controller. The solution is a VC operating system, that offers solutions for venture capitalists (VC’s) to source, screen and manage their deals, manage their investment portfolio, produce investor updates and reports, and other fund operation and investor tools, depending on the modules used by the Data Controller.

C.2. Security of processing

The level of security considers that the processing involves confidential personal data which is why a ‘high’ level of security should be established.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security. The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

General security measures
The data processor must ensure that:

- All employees who have access to personal data have committed themselves to confidentiality, either by agreement or pursuant to legislation, in relation to personal data and processing activities, and that such confidentiality obligation also applies after the termination of the parties' co-operation and after the employee's employment with the data processor has ended
- All employees of the data processor who have access to personal data are subject to internal policies for IT security and data protection
- All employees of the data processor who have access to personal data are regularly trained in IT security and data protection
- Systems used by the data processor for the processing of personal data are based on data security and best practices in data protection

Organisational security measures
The data processor must ensure that:

- Physical locations from which personal data is processed are protected with intrusion protection
- Access to physical locations from which personal data is processed can only take place via a personal key card or other access control measure
- Visitors who gain access to physical locations from which personal data is processed are not left unattended.

Encryption of personal data
The data processor must ensure that:

- All transmission of sensitive and confidential personal data over the internet (e.g. via e-mails and the platform) takes place via a sufficiently encrypted connection
- Equipment used for the processing of personal data is encrypted.

Ensuring ongoing confidentiality, integrity, availability, and resilience
The data processor must ensure that:

- Only the data processor's authorised employees have access to personal data
- The data processor's employees only have access to personal data to the extent necessary for the performance of their work and the purpose of the processing
- All employees have unique usernames and passwords
- Password policies have been implemented to ensure that passwords are sufficiently strong and are changed regularly
- Equipment provided to the data processor's employees for use in the performance of their work must be secured with access control
- Employees are required to maintain access control and ensure that passwords remain personal and confidential
- Procedures must be implemented to ensure that employees lock their screen when leaving it, and automatic screen lock must be implemented which activates after a short period of inactivity
- A well-functioning backup is established and that regular spot checks are carried out to ensure that backups are completed
- Access to systems used for processing personal data is secured with individual confidential passwords
- Procedures are implemented to protect against malicious events in operational equipment
- Procedures are implemented to prevent the destruction, loss, alteration, or unauthorised disclosure of personal data stored on electronic and physical equipment
- Operational servers only have necessary services and ports open and are regularly updated for security
- Firewalls and anti-virus programmes are used on all equipment used for processing personal data, and that firewalls and anti-virus programmes are updated at all times
- Remote access to personal data by employees, including in connection with working from home, is in accordance with the points in this section.

Logging
The data processor must ensure that all access to and processing of personal data is logged, including systems, databases, platforms, devices etc.

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:

Assistance subject to Clause 9.1
In the event that the data processor receives requests concerning data subjects' rights relating to the data controller's personal data, the data processor shall, without undue delay, transmit the requests via an encrypted connection to the data controller.

The data processor shall implement the necessary technical and organisational measures so that the data processor can assist the data controller in securing and fulfilling the data subjects' rights.

The data processor shall, without additional charge, ensure that solutions used for processing the data controller's personal data make it possible to fulfil the data subjects' rights under the GDPR. This means, among other things, that the data processor must ensure that it is possible to fulfil data subject requests and that the solution must therefore be able to deliver all personal data relating to a specific data subject in PDF format via a secure communication connection to the data controller. Alternatively, in the event that such technical solution does not exist, the data processor shall provide the same functionality manually.

The data processor may charge a fee, based on the data processors regular consultancy fees, for assistance with ensuring compliance with the data controller's obligation to fulfil data subjects' requests within the time limit set out in the GDPR.

Assistance subject to Clause 9.2
In accordance with Clause 9.2 and Section 10 of these Clauses, the data processor shall - taking into account the nature of the processing and the information available - assist the data controller in notifying the supervisory authority of the breach by providing the following information:

a) A description of the incident, including where it physically occurred
b) A sequence of events, including information about the start, detection and (expected) termination of the event
c) The nature of the personal data breach, including any technology involved, the categories of data and data subjects, as well as the approximate number of data subjects affected and, if possible, the approximate number of records
d) a general assessment of the likely impact on data subjects
e) A description of the measures taken by the data processor and/or proposed to be taken by the data controller to address the incident and mitigate the adverse effects of the breach
f) Indication that the notification is final or whether and how further information will follow
g) Indication of where the data controller can obtain further information.

If it is not possible to provide all the information mentioned above at once, the information shall be provided progressively, without undue delay and after it becomes possible for the data processor to obtain the information.

The data processor is obliged to actively contribute to ensuring that the data controller receives sufficient information to fulfil any obligation to inform the competent supervisory authorities and the data subjects of the personal data breach.

The notification of a personal data breach as well as the above information shall be sent in writing as an e-mail marked as "high priority" to the data controller.

The data processor shall not make any public statements or statements to third parties about personal data breaches without prior written agreement with the data controller.

C.4. Storage period/erasure procedures

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

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the data processor's own premises, sub-processors' premises, cf. Appendix B.2 and work from home workplaces in accordance with the data processor's and sub-processor's policies.

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

The data processor may transfer personal data to recipients outside the EU/EEA ("third countries") using the legal transfer mechanisms provided for in Chapter V of the GDPR, including, inter alia, the EU Commission's Standard Contractual Clauses (SCCs), the EU-U.S. Data Privacy Framework and transfers to safe third countries that have received an adequacy decision from the EU Commission.

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 controller or a representative of the data controller shall at appropriate intervals carry out an inspection of the data processor's compliance with this data processing agreement.

The parties agree that, because of the nature of the processing and the content of the personal data, audits may be carried out using management statements or questionnaires.

Depending on the results of the audits, the data controller is entitled to request the implementation of additional measures in order to ensure compliance with the GDPR, data protection provisions of other EU or Member State law and these Clauses. Additional security measures are agreed separately and are subject to the data processors consultancy fees and potential implementation costs.

Any costs incurred by the data controller in connection with any audits shall be borne by the data controller itself. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the data controller to carry out its supervision.

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

The data controller or a representative of the data controller shall at appropriate intervals carry out an inspection of the data processor's compliance with this data processing agreement.

The data processor or a representative of the data processor shall, at appropriate intervals, conduct written, or physical audits of the sub-processors associated with the agreement in order to determine the sub-processor's compliance with the data protection legislation and these Clauses.

Based on the results of such an audit, 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. Additional security measures are agreed separately and may be subject to additional fees.

Documentation for such inspections shall, at the request of the data controller, be submitted to the data controller for information.

8. Appendix D The parties’ terms of agreement on other subjects