AMESTO PAYROLL

Standard Contractual Clauses

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

Amesto Accounthouse A/S
CVR nr. 26113156
Vandtårnsvej 62a, 4. Sal
2860 Søborg

Hereinafter referred to as (The data processor) and the customer, hereinafter referred to as (The data controller), each a 'party'; together 'the parties'.

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

1. 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 regards 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 payroll and accounting services 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. One appendix is attached to the Clauses and form an integral part of the Clauses.

6. The Agreement contains the data controller's instructions with regards to the processing of personal data and 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 A contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.

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

9. 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.

2. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

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

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

3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions are specified in The Agreement. 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.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor,

contravene the GDPR or the applicable EU or Member State data protection provisions.

4. CONFIDENTIALITY

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

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

5. 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 organizational measures to ensure a level of security appropriate to the risk.

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

a. Pseudonymization 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 organizational measures for ensuring the security of the processing.

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

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

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.

6. USE OF SUB-PROCESSORS

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

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

3. The data processor has the data controller's general authorization for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorized by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the 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 organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

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

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.

7. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

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

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

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

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

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

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

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

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.

8. ASSISTANCE TO THE DATA CONTROLLER

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the 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 national supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the data controller's obligation to communicate without undue delay 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 national supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

In the Appendix to The Agreement, the parties have defined the appropriate technical and organizational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

9. 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 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.

10. ERASURE AND RETURN OF DATA

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to 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.

The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

11. AUDIT AND INSPECTION

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

2. The controller may, at its own expense and at any time, check the performance of the processing and the fulfilment of the obligations imposed on the processor by the clauses. The audit shall be carried out in such a way as not to jeopardize in any way the obligations of the processor towards third parties or the authorities.

The audit shall be limited to assessing whether the data processor is complying with its obligations under the clauses and shall not reveal information about other customers held by the data processor or data relating to the application of security measures by the data processor.

Any representative of the controller or external auditor participating in the audit shall be subject to the usual obligations of confidentiality towards the data processor.

3. Unless required by legislation, audits shall not be carried out more than once in any twelve (12) month period. The controller shall bear all audit costs and shall compensate the processor for any costs incurred as a result of the audit.

The data processor shall be obliged to grant access to the data processor's physical facilities to supervisory authorities which have access to the controller's or processor's facilities under applicable law, or to representatives acting on behalf of the supervisory authority, upon presentation of appropriate identification.

12. 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.

13. 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.

14. SIGNATURE

The data processor can be contacted via the contact person below.

Denmark
Name Nadia Dyg

Titel	Operations Manager
Phone No.	**+45 70 229 299**
E-mail	**gdpr@accounthouse.dk**

Norge

Name	Torstein Heggen
Titel	Privacy Manager, Amesto Group
Phone No.	**+ 47 922 03 214**
E-mail	**torstein.heggen@amesto.no**

Sverige

Name	Sofia Gonzales
Titel	Local Privacy manager
Phone No.	+ 46 8 669 60 00
E-mail	sofia.gonzalez@amesto.se

APPENDIX A APPROVED SUB-PROCESSORS

Upon entry into the Agreement and the clauses, the controller has authorized the use of the following sub-processors.

Processor	**Location**	**Legal basis for processing outside the EU/EEA**	**Purpose**
XDC	EU/EEA		Hosting and IT services
Firstpoint	EU/EEA		IT services
OneFlow	EU/EEA		E-signing
Citrix	EU/EEA		Privacy and compliance
eMarketeer	EU/EEA		E-mail marketing
Microsoft	USA	SCC	E-mail and hosting
Penneo	EU/EEA		Legal Compliance
Visma	EU/EEA		Invoicing, payroll and accounting
Google	EU/EEA		Marketing and statistics
Facebook	USA	SCC	Marketing and statistics
Lessor	EU/EEA		Payroll
TimeLog	EU/EEA		WTR and invoicing
Hubspot	USA	SCC	CRM
Xledger	EU/EEA		Accounting
Mertaoja OY	EU/EEA		Payroll

Processor	Location	Legal basis for processing outside the EU/EEA	Purpose
CC Interactive	EU/EEA		Automation
Stråhlfors A/S	EU/EEA		Communication and distribution
Filezilla	EU/EEA		Communication and distribution

Upon entry into the Agreement and the clauses, the controller has authorized the use of the above-mentioned sub-processors for the processing activity described. The processor may not – without the written consent of the controller – make use of a sub-processor for a processing operation other than that described and agreed or make use of another sub-processor for that processing operation.

Subcontractors to Amesto AccountHouse A/S may gain access to personal data when the Customer enters into an agreement with the Data Processor for the provision of services. The subcontractors provide services and performances that the Data Processor deems necessary to fulfill the contractual obligations and the agreement entered with the Customer.

The list will be continuously updated, and all Clients will also be notified in advance of any changes.

APPENDIX B: INFORMATION ABOUT THE PROCESSING

The information about the processing of data is specified according to the following services:

A: Payroll services
B: Accounting services

A.1. The purpose of The Data Processor's processing of personal data on behalf of The Data Controller is:

Processing of the data is necessary to fulfill the contract between The Data Processor and The Data Controller.
The purpose of the processing is payroll administration and additional services in relation to payroll administration as agreed upon in the Contract or otherwise requested in writing by The Data Controller.

B.1. The purpose of The Data Processor's processing of personal data on behalf of The Data Controller is:

Processing of the data is necessary to fulfill the contract between The Data Processor and The Data Controller.
The purpose of the processing is bookkeeping and additional accounting services in relation to financial administration as agreed upon in the Contract or otherwise requested in writing by The Data Controller.

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 nature of the processing includes, but is not limited to, handling the monthly payroll input including mileage, taxable benefits, insurance, and pension funds. Ensure payments of holiday allowances, deduction of holidays, retrieve and declare employee taxes, distribute paychecks through Nets/e-Boks and prepare payroll reports.

B.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 nature of the processing includes, but is not limited to, finance bookkeeping, invoicing, monitoring and control of accounts receivables, handling monthly depreciations, preparation and filing of VAT returns, assisting with year-end tasks and preparation of Financial Statement / Annual report in conjunction with appointed auditor.

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

- Information in connection to the customer relationship
- Information related to payroll administration, reimbursements, and HR services

The following enumeration is non-exhaustive, as the type of data processed depend entirely on the services acquired by The Data Controller:

Name, e-mail address, telephone number, address, social security number (CPR), payroll and tax information (e.g., salary, commissions, pension, insurance, membership of trade unions, taxable benefits, company car etc.) payment details, workplace address, employment information e.g., job title, payroll seniority, holdings in the company, employment start/end, collective agreements, absence and leaves etc.

In addition, The Data Processor will only process other relevant data that is strictly required in order to perform the services as described in the Contract or explicitly requested by The Data Controller in writing.

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

- Information in connection to the customer relationship
- Information related to accounting and bookkeeping services

The following enumeration is non-exhaustive as the type of data processed depend entirely on the services acquired by The Data Controller:

Name, contact information, payment details, assets in cohabitation, criteria in shareholder agreements, bank account number, tax deductions, salary levels, financial conditions, role in Company, behavioral patterns (receipts) etc.

In addition, The Data Processor will only process other relevant data that is strictly required in order to perform the services as described in the Contract or explicitly requested by The Data Controller in writing

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

Current and former employees of The Data Controller as well as company contacts.

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

Company contacts, debtors and creditors and occasionally current employees 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:

Processing shall not be limited and shall therefore be performed until the Contract is terminated by either party, unless otherwise agreed upon in the Contract (Temp agreement or other type of time limited agreement)

B.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:

Processing shall not be limited and shall therefore be performed until the Contract is terminated by either party, unless otherwise agreed upon in the Contract (Temp agreement or other type of time limited agreement)

APPENDIX C: INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

The instruction pertaining to the use of personal data is specified according to the following services:

A: Payroll services
B: Accounting services

A.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 processing required in order to fulfill the contractual obligations and services acquired by The Data Controller.
The following enumeration is non-exhaustive as the type of data processed depend entirely on the services acquired by The Data Controller.

- Set up a payroll schedule for the employee
- Review input
- Collect tax information
- Calculate gross pay
- Determine and handle deductions – taxes, pension funds, insurance etc.
- Exchange data with required public authorities
- Calculate net pay
- Simulate payslips for approval
- Issue payments
- Keep payroll records
- Handle miscalculations, mistakes, or delayed input
- Payroll reporting
- Apply for reimbursements
- Resign employees in payroll system, pension funds, insurance etc.

B.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 processing required in order to fulfill the contractual obligations and services acquired by The Data Controller.

The following enumeration is non-exhaustive as the type of data processed depend entirely on the services acquired by The Data Controller.

- General finance bookkeeping
- Balance reconciliations
- Payments of accounts payable
- Invoicing
- Follow up on, monitoring and control of accounts receivables
- Intercompany re-charges
- Preparation and filing of VAT returns on a regular basis
- Filing of payroll, social securities, and relevant income taxes
- Fixed Assets accounting and bookkeeping of monthly depreciations
- Preparation of trial balance
- Preparation of management reporting
- Year End tasks concerning the financial year
- Preparation of Financial Statement

C.2. Security of processing

The Data Processor's level of security shall always take into account the nature, scope, context, and purpose of the processing as well as the risk for the rights and freedoms of natural persons. The following enumeration of elements, that are essential to The Data Processor's level of security is independent of the services acquired by The Data Controller.

Regardless the services acquired by The Data Controller, the processing of data on behalf of The Data Controller involves a large volume of personal data and/or business-critical information, which is why a 'high' level of security is established.
The Data Processor is entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary level of data security.

The Data Processor shall however – in any event and at a minimum – implement the following measures:

- Protect data in transit and data at rest with AES 256-bit encryption where possible.
- All electronic access require a personal user ID and password.
- All access is limited on a need-to-know basis
- No data or documents are stored in printed form.
- Printed documents are discarded securely in locked shredding containers

- Confidentiality is ensured through NDA's, employment contracts, sworn statements and data processing agreements with employees, subcontractors, and partners.
- Ensure integrity, availability and resilience of processing systems and services through continuous risk assessments, audits, and inspections of sub processors and internally – annually or as required.
- Ensure ability to restore and access personal data within 12 hours in the event of an incident.
- Conduct testing, assessing, and evaluating the effectiveness of the applicable technical and organizational measures annually or as required, to ensure the security of the processing.
- Only permit access to data online only through Remote Desktop Protocols and two-factor authentication (when possible)
- Only permit access to physical locations where data is processed to employees and visitors accompanied by employees.
- Conduct internal audits and provide employees with education and security policies to ensure that remote working is compliant with the abovementioned requirements
- Monitor and log all processing of data to the extent possible. Logged incidents must be reviewed, handled and documented instantly as well as controlled at least annually.

C.3. Assistance to The Data Controller

The Data Processor will insofar as this is possible – within the scope and the extent of the Contract, assist The Data Controller in accordance with GDPR Clause 9.1. and 9.2.
Therefore, The Data Processor has implemented the following measures:

- The Data Processor will at all times refuse receipt of data from The Data Controller revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation – unless such information is relevant to the fulfillment of the Contract and/or the services acquired by The Data Controller.
- The Data Processor is responsible, among other, for assisting The Data Controller in ensuring that the processing of personal data, which is instructed by The Data Controller, has a legal basis. The Data Processor will immediately inform The Data Controller if instructions given, contravene the GDPR or the applicable EU or Member State data protection provisions.

- The Data Processor does not respond to or resolve a request from an employee on their rights, including insights, but passes the query on to The Data Controller as soon as possible.
- The Data Processor can upon specific request assist The Data Controller in their compliance with the data subjects' rights and notification obligations. The Data Processor is, however, entitled to be compensated for its employee's time used on assisting The Data Controller.
- In the event of a data breach, The Data Processor will assist The Data Controller, with all the information available to The Data Processor, in order for The Data Controller to assess the extent of the breach, report the breach to the supervisory authority if necessary and notify the data subject.
- The Data Processor can, if requested, assist The Data Controller with the reporting of a breach to a supervisory authority and the notification of the breach to the data subject. The Data Processor is, however, entitled to be compensated for its employee's time used on assisting The Data Controller.

C.4. Storage period/erasure procedures

Upon termination of the Contract, The Data Processor shall return all personal data to The Data Controller and delete existing copies unless otherwise required under national law. The Data Processor commits to exclusively processing the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

Personal data is stored for 5 years after termination of the Contract according to obligations under national law.

C.5. Processing location

The processing of personal data will be performed as required by The Data Controller at the designated business address, The Data Processor's offices or external locations approved by The Data Processor (e.g., home workspaces).

If the work is performed mainly at The Data Controller's address, control, and documentation work as well as planning and organization, will also have to be performed at The Data Controller's address.

The Data Processors servers and back-up servers are located at two different locations within the EU/EEA.

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

The Data Processor and its sub-processors (if any) may transfer Personal Data out of the territory of the member states of the European Union, the European Economic Area, or other countries which the European Commission has found to guarantee an adequate level of data protection (collectively, the "Approved Jurisdictions"), upon thirty (30) day's prior written notice to the Data Controller, to the extent the Data Controller does not object to the transfer in writing within such notice period.

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 will comply with reasonable requests made in writing by the Data Controller to audit the Data Processor's Processing activities necessary to enable the Data Controller to verify that the Data Processor is complying with its obligations. The Data Controller shall bear all audit expenses and compensate the Data Processor for any and all costs incurred as a result of the audit. Unless required by Privacy Laws, any audits will be conducted no more than once in any twelve (12) months period.

Internal Audits and inspections are made continuously to ensure, that all relevant policies and guidelines are complied with. Based on the results of the internal audits/inspections, The Data Processor revises the relevant policies and guidelines and may implement additional measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

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 at the data processor's expense carry out an inspection concerning the sub-processor's compliance with this data processing agreement.

The data processor or the data processor's representative shall have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data processor deems it necessary.

Documentation for such inspections of the sub-processors shall upon request be sent to the data controller.