Data processor agreement

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

between

The Client

(the data controller)

and

The Accounting firm

(the data processor)

each a ‘party’; together ‘the parties’. For an overview of which legal entities are covered by "The Accounting Firm", see appendix D.

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 accounting and payroll services, as well as related 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. 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. The sections marked with "*" in these Terms and Conditions have supplementary provisions in Appendix D.

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

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

3. The rights and obligations of the data controller

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

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

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

4. The data processor acts according to instructions*

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

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

5. Confidentiality

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

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

6. Security of processing*

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural

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

persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

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

a. Pseudonymisation and encryption of personal data;
b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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

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

   If subsequently – in the assessment of the data controller – mitigation of the identified risks 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 7 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)*.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing

sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

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

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

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

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

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

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
    a. transfer personal data to a data controller or a data processor in a third country or in an international organization
    b. transfer the processing of personal data to a sub-processor in a third country
    c. have the personal data processed in by the data processor in a third country

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

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

9. Assistance to the data controller*

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

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:
   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:
   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
   d. the data controller's obligation to consult the competent supervisory authority (see Appendix D), 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 72 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.

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.

2. For an overview of EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services, see Appendix D
   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.

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.

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 data processor shall notify the data controller without undue delay if it is discovered that the data controller does not fulfill its obligations in this data processing agreement, or if it is likely that the data controller will not be able to fulfill them.

2. The data controller must indemnify the data processor for all claims, expenses, losses and liabilities that arise in connection with the data controller's breach of the Clauses or privacy legislation.

3. Appendix D contains additional provisions that elaborate on certain sections of the Clauses

14. Commencement and termination

1. 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.

2. 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.

3. 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.

Appendix A Information about the processing

The purpose of data processing is accounting and payroll services, as well as associated advisory services. Such associated advisory services may include, but are not limited to, consulting services and delivery of IT systems. Please see the main agreement for for details of the processing.

The processing lasts until the end of the assignment contract.
Please note. The storage times starts counting from the first year-end after the personal information has been processed

Type of services	Personal data	Purpose	System	Categories of data subjects	Storage time
All clients	All documentation related to assignments that are received from or sent to clients (see specifics for services), or prepared by Amesto	Delivery of services, including communication and storage of documentation	PowerOffice, MyAmesto, Citrix, Microsoft Office 365	Contact persons, client's employees, client's customers and suppliers	5 years
All clients	Information needed for handling support cases. May contain same type of information as the specifics for services, but we limit the personal information as much as possible	IT Support Services	SuperOffice	Contact persons, client's employees, client's customers and suppliers	5 years
Accounting services	Name	Identification	All systems	System users, references on vouchers, business owners with personal liability, persons with expense accounts	5 years
Accounting services	Contact information, including organiational affiliation	Identification, login to systems, administration and reporting	All systems	System users, references on vouchers, business owners with personal liability, persons with expense accounts	5 years
Accounting services	Information in vouchers. May be name, bank account number, organisational affiliation and other information.	Accounting of vouchers	ERP-systems, reconciliation systems	Voucher references, business owners with personal liability, persons with expense accounts	5 years
Accounting services	Social security number	Identification	Annual settlement systems (financial and tax), shareholder registeres	Business owners with personal liability, shareholders	5 years
Accounting services	Salary information and personal economy	Tax return	Annual settlement systems (financial and tax)	Business owners with personal liability	5 years
Accounting services	Health information	Tax return	Annual settlement systems (financial and tax)	Business owners with personal liability	5 years

Accounting services	Family information	Tax return	Annual settlement systems (financial and tax)	Business owners with personal liability	5 years
Accounting services	Bank account number	Tax return	Annual settlement systems (financial and tax), shareholder register	Business owners with personal liability, shareholders	5 years
Accounting services	Union affiliation	Tax return	Annual settlement systems (financial and tax)	Business owners with personal liability	5 years
Payroll and HR services	Name and employee number	Identification, payroll and HR services	All systems	Employees	5 years after the employment has ended
Payroll and HR services	Contact information, including but not limited to telephone number, email address, postal information	Identification, login to systems, payroll and HR services	All systems	Employees	5 years after the employment has ended
Payroll and HR services	Organizational affiliation	Administrative purposes and reporting	All systems	Employees	5 years
Payroll and HR services	Social security number	Identification, public reporting	Payroll systems, reconciliations	Employees	5 years after the employment has ended
Payroll and HR services	Bank account number	Payments	Payroll systems, reconciliations	Employees	5 years
Payroll and HR services	Salary and other salary related information	Payroll and HR management	Payroll systems, reconciliations	Employees	5 years
Payroll and HR services	Information regarding sick leave	Payroll and HR management	Payroll systems, reconciliations	Employees	5 years
Payroll and HR services	Information regarding other leaves and absence	Payroll and HR management	Payroll systems, reconciliations	Employees	5 years
Payroll and HR services	Union affiliation	Payroll	Payroll systems, reconciliations	Employees	5 years
Payroll and HR services	Employee contracts	Payroll and HR management	Payroll systems, reconciliations	Employees	5 years after the employment has ended
Payroll and HR services	Documentation related to HR management, including employee contracts, warnings, resignations, dismissals, etc.	HR management	Payroll systems, reconciliations	Employees	5 years after the employment has ended
Payroll and HR services	Working hours	Payroll, HR management, financial controlling	Payroll systems, reconciliations	Employees	5 years
Payroll and HR services	Information from travel expenses and other expenses	Payroll	Payroll systems, reconciliations	Employees	5 years
Other services	Name	Identification	All systems	Contact persons, tenants, securities owners	Follows other storage requirements
Other services	Contakt information	Identification, login	All systems	Contact persons, tenants, securities owners	Follows other storage requirements

Appendix B Systems, and authorised sub-processors

All sub processors does not apply for all clients. The table shows all sub processors that may be in use, depending on which services the data processor delivers, and on which system(s). The systems/sub processors defined under All services (Type of services) may apply for all clients.

*All systems with On premis storage, have storage within our Citrix platform hosted by Visma IT & Communications AS. The sub processor may have access to the data when working on support cases

** Data is stored in EU/EEC, but sub processor is owned or is using systems owned by American companies. This is considered transfers to third countries. Standard Contractual Clauses approved by the EU Commission applies.

Type of services	System	Type	Sub processor	Storage
All services	All systems	Group company. Used for joint customers and for assistance in carrying out assignments	Alfa økonomi AS	See system spec.
All services	All systems	Group company. Used for joint customers and for assistance in carrying out assignments	Amesto AccountHouse A/S	See system spec.
All services	All systems	Group company. Used for joint customers and for assistance in carrying out assignments	Amesto AccountHouse AB	See system spec.
All services	All systems	Group company. Used for joint customers and for assistance in carrying out assignments	Amesto AccountHouse AS	See system spec.
All services	All systems	Group company. Used for joint customers and for assistance in carrying out assignments	Amesto AccountHouse Drammen AS	See system spec.
All services	All systems	Group company. Used for joint customers and for assistance in carrying out assignments	Amesto AccountHouse Østfold AS	See system spec.
All services	Citrix	Servers/databases for our on-premise applications	Visma IT & Communications AS (NO/SE) XDC Gruppen (DK)	EU/EEC
All services	ConnectMyApps	System integrations	ConnectMyApps AS	EU/EEC
All services	Dib	Consulting services	DIBKunnskap AS	EU/EEC

All services	Econominds	Accounting consultancy	Econominds ApS	EU/EEC
All services	FileZilla	File Exchange	XDC Gruppen	EU/EEC
All services	Office 365, including SharePoint and Power BI	Communication, file exchange, file storage	Microsoft Norge AS, Microsoft Danmark A/S	EU/EEC**
All services	Monday work management	Project management for implementation projects	Monday.com	USA (name, e-mail & logon logs only)
All services	MyAmesto	Communication, file exchange	Microsoft Auth(0) Inc (authentication only) Mailgun Technologies, Inc (send notifications only)	EU/EEC**
All services	PowerOffice Win	Storage of documentation	PowerOffice AS	On premis*
All services	Ricoh Smart Integration	Printing, copying and scanning of documents	Ricoh Norge AS	EU/EEC and approved third countries (UK and Japan)
All services	SFTP	File Exchange	WinSCP	EU/EEC
All services	ShareFile	Communication File exchange	Amesto Solutions AS	EU/EEC
All services	Sticos	Consulting services	Sticos AS	EU/EEC
All services	SuperOffice	Amesto internal and external IT support	Amesto TechHouse AS	On premis*
Accounting services	All systems	Accounting services in Finland	AddValue Advisors OY	EU/EEC
Accounting services	Amesto Analyse	Reporting	Amesto Solutions AS	On premis*
Accounting services	BL Bokslut	Accounting	Visma IT & Communications AS	On premis*
Accounting services	BL Skatt	Accounting	Visma IT & Communications AS	On premis*
Accounting services	Cantor controller årsoppgjør	Annual settlement system	Cantor AS	EU/EEC
Accounting services	CaseWare	ERP System	Administrationsselskabet af 15. marts 2015 ApS	EU/EEC
Accounting services	e-conomic	Visma e-conomic A/S	ERP-system	EU/EEC
Accounting services	Escali	Investments handling	Visma IT & Communications AS	On premis*
Accounting services	Fenistra	Financial property management	Fenistra AS	On premis* EU/EEC
Accounting services	Finale products	Annual settlement system and reporting	Visma IT & Communications AS	On premis*

Accounting services	Fortnox	ERP System	Fortnox AB	EU/EEC
Accounting services	Hogia Bokslut	ERP System	Hogia	EU/EEC
Accounting services	Hogia Skatt	Tax return	Hogia	EU/EEC
Accounting services	Letregnskab.dk	Audit of financial statements	Letregnskab.dk ApS	EU/EEC
Accounting services	Mertaoja	Accounting services in Finland	Talouskonsultointi Mertaoja Oy	EU/EEC
Accounting services	Navision	ERP system	Microsoft Danmark A/S	EU/EEC
Accounting services	Netaccount	ERP system	Netaccount Regnskap AS	EU/EEC
Accounting services	OneStopReporting	Reporting	Visma Software AS	EU/EEC
Accounting services	On-Property	ERP System, financial property management	On Property AS	EU/EEC
Accounting services	PowerOffice Go	ERP System	PowerOffice AS	EU/EEC
Accounting services	Semine	ERP System	Semine AS	EU/EEC
Accounting services	Total Årsoppgjør	Annual settlement system	Visma Software AS	On premis*
Accounting services	Tripletex	ERP System	Tripletex AS	EU/EEC
Accounting services	Uni Regnskap / Uni Fakturering	ERP System	Unimicro	EU/EEC
Accounting services	Visma Business	ERP System	Visma IT & Communications AS	On premis*
Accounting services	Visma Global	ERP System	Amesto Solutions as	EU/EEC
Accounting services	Visma Periode & År	Annual settlement system	Visma Software AS	EU/EEC
Accounting services	Visma.net Financials and other Visma web products	ERP System	Visma Software AS	EU/EEC
Accounting services	Wolters Kluwer	Financial statements and tax return	Wolters Kluwer Danmark A/S	EU/EEC
Accounting services	Xledger	ERP System	Xledger AS	EU/EEC
Payroll and HR services	Account Control	Reconciliations	Save Solutions AS	
Payroll and HR services	All systems	Payroll services in Finland	AddValue Advisors OY	EU/EEC
Payroll and HR services	Corell Consult	Payroll administration in Lessor PM5	Corell Consult	EU/EEC
Payroll and HR services	Danløn	Payroll	Danske Lønsystemer	EU/EEC
Payroll and HR services	Flex HRM	Timesheets, travel expenses, HR, Payroll	Flex Applications Sverige AB	EU/EEC
Payroll and HR services	Flex Portal	Timesheets, HR Services	Amesto AccountHouse AB	EU/EEC
Payroll and HR services	Fortnox	Payroll system	Fortnox AB	EU/EEC

Payroll and HR services	Hogia PBM	Time sheets,	Hogia	EU/EEC
Payroll and HR services	Hogia Travel	Travel expenses	Hogia	EU/EEC
Payroll and HR services	Hogialön+	Payroll system	Hogia	EU/EEC
Payroll and HR services	HR Manager		HR; Talent Solutions ApS	EU/EEC
Payroll and HR services	Lessor	Payroll system	Lessor A/S	EU/EEC
Payroll and HR services	Lessor Portal	Payroll system	Lessor A/S	EU/EEC
Payroll and HR services	Mertaoja	Payroll services in Finland	Talouskonsultointi Mertaoja Oy	EU/EEC
Payroll and HR services	Uni Lønn	Payroll system	Unimicro	EU/EEC
Payroll and HR services	Visma Lønn	Payroll system	Visma IT & Communications AS	On-premis*
Payroll and HR services	Visma.net and other Visma web products	Payroll system	Visma Software AS	EU/EEC
Payroll and HR services	Xledger	Payroll system	Xledger AS	EU/EEC
Payroll and HR services	Zenegy	Payroll system	Zenegy Danmark ApS	EU/EEC** (Microsoft Azure)
Payroll and HR services		Payroll system	Mertaoja	

Appendix C Instructions 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:

Registration and payment of vouchers, registration and payment of payroll, registration and payment of travel and expense bills, internal and public reporting, advisory services, IT services and other related services. The specifics of the activities are stated in the assignment agreement.

C.2. Security of processing

The level of security shall take into account that the processing may involve confidential and special catgetories of personal data (ref. Article 9 GDPR), depending of the scope of the assignment. Confidential information may be social security number, salary, bank account numbers, etc. Special categories may include trade union membership and health information (sick leaves, etc.).

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 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:

All systems require personal logon with password.

All systems containing confidental information have muliti factor authentication logon

All computers may be remotely locked and erased by IT department.

All employees must annualy complete a security awareness program.

Access to systems, mail, etc. via phones, pads, etc, have the same security measures as computers.

Data is encrypted during transfer.

There is access control at all locations, and all data centeres have a high level physical access control

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.

The data subjects primary contact is the data controller. If the data processor is contacted by the data subject with regards to Clause 9.1, the data processor will forward the request ot the data controller. The data processor will assist the data controller in the data controller's compliance with the rights mentioned in Clause 8.1. The data controller will invoice such assistance according to the current price list. Such request from the data controller may be adressed to the data processor's regular case handler, or through the form found on Amesto Trust Center (https://www.amesto.com/amesto-trust-center/security/notification/).
If the data controller does not assist the data subjects in compliance with GDPR, and the data processor is obliged to assist the data subject according to the same legislation, the data controller will invoice the data controller according to the current price list. The data processor will inform the data controller of such assistance, and will give the data controller a reasonable amount of time to assist before the data processor starts assisting the data subject.

In the event of a personal data breach, the data processor will assist the data controller with gathering information and documentation relating to the breach, including information about what kind of information and which data subjects are involved, to whom the information is, or may be, exposed to, the nature of the breach, etc. The data processor's assistance will be invoiced according to the current price list, unless the breach is caused by conditions at the data processor.

C.4. Storage period/erasure procedures

Storage period is stated in Appendix A.

The personal data will automatically be erased by the data processor at the end of the storage period.
Upon termination of the provision of personal data processing services, the data processor shall either return and delete 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.

C.5. Processing location

Processing of the personal data under the Clauses are carried out according to appendix B

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

Personal data may only be transfered by data processor to third countries after instructions given by data controller.

Personal data may only be transfered to third countries or organisations that the Commission consider to have an adequate level of protection, or with third parties that oblige to Standard contractual clauses for data transfers between EU and non-EU countries (or similar contracts).

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 at its own expense at least every second year, the first 2023, obtain an auditor's report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.
The report is sent to the data controller upon request. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

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

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

Appendix D The parties' terms of agreement on other subjects

No.	Reference	Terms/specifications
D.1.	Parties	The client: see assignment agreement between the Client and the Accounting firm Accounting Firm: Amesto AccountHouse AS, 957 170 005 Amesto AccountHouse Sør AS, 912 976 904 Amesto AccountHouse Østfold AS, 898 709 752 Alfa Økonomi AS, 987 774 223
D.2.	Contact info	Information regarding changes in this data processor agreement will be given in MyAmesto.
D.3.	3.1.	If the data controller demands that the data processor must change or stop a processing or using a system, the data processor must be given a reasonable amount of time to comply with the controller's requirements. If the data processor is unable or unwilling to comply with the data controller's requirements, the data processor may terminate the assignment agreement. In such an event, the main agreement's regulation regarding the termination of the assignment take effect.
D.4.	3.2.	If the data processor consider an instruction from the data controller is in violation of legislation or regulations, the data processor may refuse to carry out those instructions.
D.5.	4.	If the data subject or the authorities make an inquiry related to the personal data, the data processor shall inform the data controller of such inquiries, unless the legislation or regulations prevent this. All representatives of the data controller, including external controllers who participate in audits or receive information from the data controller in accordance with this data processor agreement, are subject to a duty of confidentiality, unless the law requires authorities or the data subject to be informed.
D.6.	6.	The data processor offers a set of standardized information on information security. If the data controller needs information / documentation in addition to the data processor's standard documentation, the data processor will invoice such assistance in accordance with the current price list.
D.7.	5.3.	If the data processor is unable or unwilling to fullfull the data controllor's additional requirements, the data processor may terminate the assignment agreement. In such an event, the main agreement's regulation regarding the termination of the assignment take effect.
D.8.	7.3.	The information concerning the addition or replacement of sub-processors will be given in MyAmesto
D.9.	8.1.	Countries/territories and organisations that the European Commission has recognised to have an adequate level of data protection, is not considered to be third countries under these Clauses.
D.10.	9.	Assistance given to the data controller with regards to exercising data subject's rights, will by invoiced by the data processor in accordance with the current price list.

D.11.	10.1-10.2	In the event of a breach of personal data security, the data processor will analyze the incident with regards to the affects on the data controller. If the data controller is affected, the data processor will notify the data controller Notifications to the data controller shall provide a sufficient overview of the consequences of the breach for the services, as well as the corrective measures that the data processor shall implement. The notification shall be given without undue delay, and, if possible, within 72 hours afther the data processor has become aware of the personal data breach.
D.12.	11.1.	The data processor shall provide reasonable assistance in returning the personal information in a readable, accessible and commercially sensible file format. The data controller shall compensate the data processor for the reasonable costs associated with the return of personal data. After the return period, the data processor may delete the personal data without further notice, unless the agreement between the data processor and the data controller, or the legislation, requires that the personal data be stored. With respect to personal information stored on backup servers, this information shall be deleted in accordance with ordinary procedures and industry standards. When the data controller requests it, the data processor shall provide the data controller with a written confirmation that all the mentioned personal data has been returned or deleted, unless the legislation requires that the personal data be stored.
D.13.	11.2.	National laws demanding Dataprocessor's storage of personal information: Regnskapsførerloven and God regnskapsføringsskikk, hvitvaskingsloven Data processor acts as a data controller for the personal information under the mentioned legislation
D.14.	12.1.	The data controller can only use external controllers that are not competitors of the data processor.
D.15.	C.7.	The data controller shall cover all expenses that arise in connection with inspections, and the data processor is entitled to compensation for all costs that arise as a result of the inspection. The data processor's time spent for the inspection is invoiced according to standard price list. Unless the Personal Data Act so requires, no more than one inspection shall be carried out for each period of twelve months.