eKapital

Reporting Employee Share Scheme

Agreement between Azets Insight A/S

(Supplier)

&

Customer

Hereafter collectively referred to as the Parties, or separately referred to as the Party.

1. Agreement Structure and Prioritisation

Agreement consists of this main document with the following exhibits:

Exhibit 1: Agreement Terms and Guidelines for Azets Insight A/S
Exhibit 2: Data Processing Agreement

In the event of any inconsistency, the following precedence has been agreed:

1) Exhibit 2: Data Processing Agreement;
2) The general text of main document and any subsequent written addendum to Agreement; and
3) Exhibit 1: Agreement Terms and Guidelines for Azets Insight A/S.

2. Purpose and Scope of Agreement

2.1 Background

Customer has an employee share scheme for which special tax rules apply.

Supplier undertakes to provide assistance under this Agreement to prepare and carry out reporting for Customer to the Danish tax authorities (SKAT) via their portal eKapital no later than January 20th each year.

2.2 Assumptions

It is Supplier's responsibility that Customer each year is compliant with applicable legislation for reporting vested employee shares and/or subscription rights/stock options per employee to SKAT via eKapital meeting deadline.

All services must be performed in accordance with established routines, methods and using the software and systems used by the Supplier at all times.

Customer must appoint a person authorised to make decisions on behalf of Customer regarding questions that are submitted by Supplier.

Customer is obliged to deliver correct information so that Supplier can perform Services in accordance with Agreement. The required information is for the present per calendar year:

1. Information on issued/vested shares and/or subscription rights/stock options per employee in format delivered by Supplier where limited taxable employees must be marked as such;
2. eIndkomst "Sumoplysning" for each CVR-number for;
    a. "Kode68";
    b. "Feltnr. 00 36"; and
3. eIndkomst information "Feltnr. 00 36" per employee for each CVR-number/"Kode68".

Supplier must receive the information no later than December 18th each year in order to perform Services in accordance with Agreement. However, if Customer has entered into a separate written agreement with Supplier for outsourcing of payroll and Supplier is still supplying under the separate agreement, Customer grants Supplier the right to compile the above data reported in eIndkomst (item 2 and 3 above) on behalf of Customer.

Supplier's work is performed based on available information and must be performed in accordance with applicable law. Supplier must inform Customer of any relevant changes to legislation in connection with the performance of Services.

If Agreement is signed by both Parties on or before December 18th the Services for the current calendar year with reporting deadline January 20th next year will be carried out by Supplier. However, if Agreement is signed by both Parties after December 18th, this calendar year, Services will first apply for the coming calendar year with reporting deadline January 20th the year following.

2.3 Services

Supplier is responsible for delivering the following Services on a recurrent basis.

1. Yearly start-up activities in preparation for reporting to eKapital:
    - Review of material received from Customer;
    - Examination and determination of the type of share program, matching shares etc.;
    - Contact to Customer and tax authorities, if necessary;
    - Preparation of eKapital reporting data per employee; and
    - Reconciliation between eIndkomst (SKAT) and calculated eKapital reporting per employee.

2. Yearly reporting to eKapital for each individual employee.

3. Prices and Terms

3.1 Prices

All prices are in DKK excluding VAT.

Fees are as follows:

• Yearly start-up fee, if more than 10 fully taxable employees per CVR-number	DKK 5,000
• Yearly start-up fee, if less than 10 fully taxable employees per CVR-number	Based on time spent
• Yearly start-up fee for limited taxable employees	Based on time spent
• Yearly reporting to eKapital, per fully or limited taxable employee	DKK 450
• Yearly KYC-compliance fee	DKK 500

If Customer is not committed to report to eKapital for a given year, the above fees will not be invoiced as the Services are then not applicable.

Any Additional work is invoiced based on time spent at current hourly rates that presently are as follows:

• Advisory services	DKK 1,570
• Complex advisory services	DKK 2,340

Fees are added transport costs according to state tariffs (calculated from the nearest Supplier location to Customer), transport time (50% of relevant rate), parking costs and other expenses.

Prices are adjusted for inflation and wage development, etc. once a year in accordance with exhibit 2, section 12.6. The first time will be May 1, 2023.

Other terms and conditions are set out in exhibit 1, section 12.

3.2 Invoicing

Services will be invoiced on a monthly basis at the end of the month. However, the annual KYC-compliance fee is invoiced proportionally from the month in which Agreement is signed and until the next 31st December. Thereafter, the KYC-compliance fee is invoiced in advance for one (1) year at a time. The first time the following year per January 31st.

4. Duration of Agreement

The Agreement will become effective once both Parties have signed and will continue until terminated.

Either Party may terminate Agreement with six (6) months' written notice until the end of a month.

Agreement Terms and Guidelines for Cooperation with Azets Insight A/S

Supplier is a specialised provider of services within accounting, payroll administration, HR assistance, financial management, debt collection, advice, IT, and related services. Supplier does not perform legal audits.

The following guidelines, which are updated annually on May 1st, define the general framework for Agreement between Customer and Supplier unless expressly and in writing, deviated from in the main document of Agreement. The terms and guidelines in force at any time can be requested at sales_azets@azets.com or telephone +45 69 69 15 83.

The Agreement entered into between Customer and Supplier precedes these terms and guidelines.

1. Definitions

1.1 Words beginning with a capital letter not defined in Agreement have the meaning given below in both singular and plural form:

1.2 **Additional Work**: Task ordered by Customer, which is not included in SLA. Additional Work is invoiced based on time spent at current hourly rates with a minimum of ½ hour per task.

1.3 **Agreement**: This Agreement with exhibits including any data processing agreement.

1.4 **Azets Company**: Any company in the Azets Group in which Supplier is a part.

1.5 **Customer**: Any reference to Customer in Agreement includes the legal entity set forth in the main document of Agreement.

1.6 **GO-Live**: First month in which Supplier prepares reporting, payroll or similar, if this is covered by Services. In case of Agreement with a fixed term, also the month from which the term of Agreement starts.

1.7 **Party or Parties**: Customer and Supplier, as specified in the main document of Agreement.

1.8 **Reverse Service Level Agreement (hereinafter referred to as RSLA)**: Description of the tasks Customer is responsible for in accordance with the agreed delivery.

1.9 **Service Description or Service Level Agreement (hereinafter referred to as SLA)**: Description of the Services Supplier is required to provide.

1.10 **Services**: Services provided by Supplier in accordance with SLA.

1.11 **Start-up Date**: Date after the signing of Agreement, at which Supplier commences delivery of Services. Start-up date may differ from Go-Live.

1.12 **Supplier**: Any reference to Supplier in Agreement includes the legal entity set forth in the main document of Agreement.

1.13 **Working Day**: Monday to Friday, excluding public holidays, the day after Christ's Ascension, June 5, December 24, and December 31.

2. General

2.1 Customer must appoint a responsible person and a substitute who is authorised to act on matters that may be submitted by Supplier.

2.2 Supplier's employees must not have physical or electronic disposition of cash in bank or hand.

2.3 Supplier's work is carried out in accordance with written instructions from Customer. If written instructions are not received, or if such instruction is insufficient, work is carried out in accordance with Supplier's standard.

2.4 In the cooperation with Supplier and where required by law, it is the responsibility of Customer at all times to perform control of the work carried out by Supplier. Supplier cannot take over Customer's management and control responsibilities as Supplier's consultants cannot possibly have the same professional insight into Customer's operational situation and routines as Customer himself.

2.5 Supplier guarantees to carry out agreed Services according to relevant professional procedures and with professional care. However, Supplier does not guarantee to perform faultless work.

2.6 As an external accounting company (bookkeeping), Supplier is covered by the Money Laundering Act and obliged to obtain information about Customer's beneficial owners as well as having business procedures that support the Money Laundering Act and "Know Your Customer" procedures. Other customers with c/o address at Supplier are also subject to the requirements of "Know your Customer" procedures. Supplier uses an external system for storing and processing the statutory "Know your Customer" information. Customer is obliged to create and maintain the necessary data therein and otherwise contribute to Supplier meeting the requirements of the Money Laundering Act. Supplier is entitled to charge an annual fee corresponding to the direct costs associated with compliance with the Money Laundering Act.

3. Staffing

3.1 Supplier has assigned an account manager, as well as an appropriate number of consultants, so that Supplier can, to the greatest extent possible, carry out Services regardless of illness and vacation. Where it is agreed that Supplier has responsibility for instruction and control, a manager is further assigned to ensure the quality of the work performed.

3.2 Supplier appoints the consultant or consultants considered most appropriate. The wishes of Customer will influence the specific staffing.

3.3 Supplier may place the work where Supplier wishes across locations in Denmark and use Azets' Companies in Denmark or abroad to carry out part of Customer's production.

4. Physical Execution of Services

4.1 At the request of Customer, Services are carried out at specified business address or at Supplier's offices as well as at home workplaces. If Services mainly are carried out at Customer's business address, there will be regular control and documentation work as well as planning and organisation at Supplier's offices, which will result in further time spent.

4.2 Customer ensures and permits that Supplier's consultants assigned to Customer's business address have access to Supplier's e-mail and terminal server for access to Supplier's working papers, intranet, etc.

4.3 At all times, Customer's physical working conditions must comply with applicable legislation and instructions for the layout of workplaces, working environment, etc.

4.4 If Customer provides keys to Supplier's consultants, Customer is responsible for signature at receipt and return upon termination of the cooperation.

4.5 If Customer provides password and alarm codes, etc. to Supplier's consultants, Customer is responsible for changing these upon termination of the cooperation.

5. Instruction and Control Responsibilities

5.1 For Services where it is agreed that Customer has instruction and control responsibilities, it is Customer's responsibility to instruct, follow up and check the work performed by Supplier.

5.2 For Services where Supplier has instructional and control responsibility in accordance with Agreement, Supplier will regularly check the work performed by Supplier's consultants. Supplier hereby verifies that the work performed by Supplier's consultants meets Supplier's standard. If other specific controls have been agreed upon, these will be carried out in this connection.

5.3 The fact that Supplier assumes instructional and control responsibility does not limit Customer's responsibility regarding compliance with applicable legislation and for own assessment and control of payroll, accounting and accounting material, including approval of payments, payroll and related items such as pension and reporting to public authorities and the like.

6. Services Including Instruction and Control Responsibilities

6.1 Accounting

6.1.1 The work is carried out according to Supplier's standard work plan, which is adapted to Customer and updated annually or when significant changes in the Services occur.

6.1.2 Accounting includes the registration of the present vouchers in the financial, debtor and creditor ledger system etc. as well as ongoing and periodic reconciliation of accounts, where external documentation is available. For accounts where no external documentation is available, specification of relevant balance sheet items is regularly prepared. Cash and bank entries that are not documented are recorded temporarily and reclassified when documentation is available. Unless stated in SLA, accounting does not include dunning of Customer's receivables.

6.1.3 When assisting with invoicing, Customer must always check invoices/credit notes before sending them to customers. Continuous control from Customer is also necessary, where Supplier provides assistance with registration of cost of goods sold/gross margin, work in progress and stock. Supplier cannot have the necessary business insight into Customer's operation, etc. to be independently responsible for the registration and management of these areas.

6.1.4 For assistance with payment proposals, all payments must be checked, approved and executed by Customer. Customer is solely responsible for payment and the consequences thereof. Supplier cannot be held liable for any missing, incorrect or delayed payments, including the consequences of such payments, for whatever reason.

6.1.5 Supplier does not decide on continuous registration of stock or work in progress, etc., unless Customer's financial system operates specific stock/project modules, and related written instructions have been forwarded.

6.1.6 Supplier only considers accruals in accordance with Customer's instructions. Supplier, therefore, cannot guarantee correct accounting of accruals.

6.1.7 Supplier solely decides on assets and liabilities in foreign currencies, in addition to debtors and creditors, according to instructions received or by agreement. End of last month's actual exchange rate is used by default in subsequent months' registration of entries in foreign currency.

6.1.8 Depreciation, provisions and corporation tax etc. are regulated only in accordance with instructions received.

6.1.9 VAT and other taxes as well as information to the List System and Intrastat are calculated in accordance with Customer's instructions, instructions from Customer's auditor, or according to Supplier's own guidelines. If Customer is subject to special taxes of significance, Customer should provide and maintain an instruction for the area for use by Supplier. The same applies for payroll taxes (lønsumsafgift).

6.1.10 It is Customer's responsibility that VAT and tax calculation as well as reporting and payment are done in a timely and correct manner.

6.1.11 If Customer uses a financial system that is unable to print lists retroactively in time (for example stock lists) Customer himself handles the printout thereof per end date of each period.

6.2 Year-End Closing

6.2.1 By agreement, Supplier prepares the year-end closing of the books for Customer's auditor or others including the preparation of relevant working papers in the form of reconciliations of payroll related accounts, VAT and taxes, cash balances, debtor and creditor specifications and other relevant profit and loss and balance sheet accounts and related documentation.

6.2.2 The contents of a year-end closing will follow instruction from Customer, or alternatively Supplier will follow own standard.

6.2.3 If Customer fails to provide necessary documents, Supplier is not responsible for any omissions. Customer's auditor or others cannot perform the work at the expense of Supplier.

7. Payroll

7.1 Prior to agreed Go-Live Customer is obliged to establish an active Nets agreement for Supplier to use for electronic transfer of payroll payments.

7.2 **O**n a timely basis, Customer must provide the basis for payment of payrolls etc. to each of Customer's employees, including information on bonus, car and pension scheme or other. Customer must update the payroll basis whenever a change occurs

7.3 Payroll and all other payroll related payments must be checked and approved by Customer prior to Supplier's transfer to Nets.

8. Reimbursements

8.1 Supplier is informed about reimbursements to be applied for by Customer in accordance with SLA/RSLA. Regardless of the reason, Supplier may never be liable for an amount corresponding to the first 10% of the last twelve (12) months' reimbursements received. In the first twelve (12) months after Start-up Date, however, Supplier may not be liable for more than the amount Customer has paid in fees to Supplier for reimbursement applications.

8.2 Supplier cannot be held responsible for Customer's non-receipt of refunds or deviations in payment in relation to the reported reimbursement applications.

9. Storage of Material

9.1 The portion of Customer's material left in Supplier's possession under Agreement must be stored with timely care in accordance with applicable law, including the Accounting Act.

9.2 Supplier will only store physical material for the current calendar year and will then return the material to Customer. Supplier must delete digital payroll material following instructions from Customer.

9.3 At the end of a financial year or in case Agreement is terminated - except in case of breach - all physical external material will be returned to Customer after which Customer is responsible for storage. If Customer does not want the physical material returned, Supplier will invoice for storage of all material that are older than six (6) months from the beginning of the current financial year.

10. Registration Systems

10.1 Assistance is provided on Customer and/or Supplier's registration systems.

10.2 If Supplier carries out work on Customer's systems, it is Customer's responsibility to incorporate relevant restrictions in access to data. Supplier's work will follow the guidelines in the instructions received from Customer for the IT area.

10.3 Supplier or Supplier's consultants cannot be held responsible for registrations that are contained in or made in Customer's systems. Supplier does not assume any responsibility for errors that may occur in Customer's systems, regardless of whether Supplier has access to them and performs work on them, including in the event of malfunctioning.

10.4 This also applies to errors or inconsistencies in Customer's accounting and reporting, etc. arising from errors in Customer's registration systems.

10.5 Supplier has strict internal business procedures for IT use, including for the exchange of data and software, for regular backup and use of updated antivirus software. Supplier cannot accept responsibility for whether e-mails or other data media from Supplier may contain viruses or otherwise cause problems in Customer's IT systems. When spreadsheets are used, Customer must note that subsequent entry may result in changes in formulas and contexts, so manual control and recalculation is recommended before printing and using data.

10.6 Customer carries out backup routines on his own IT systems. If Supplier's consultants are involved in this, Supplier demands that Customer has an up-to-date description of backup procedures as well as a logbook where the completed backups are recorded. Supplier cannot guarantee that Customer's back-ups can be reloaded in the event of a system failure or for proper execution of the backup procedure.

10.7 If Supplier performs payroll administration on Supplier's EPOS payroll system, the assistance is performed at all times in accordance with the ISAE3402 Type II standard or a standard that may replace it.

11. Special Conditions for Systems Provided by Supplier

11.1 By using (logging on) one or more of Supplier's systems, Customer accepts the following terms and conditions:

11.2 Conditions

11.2.1 Customer is obliged at all times to ensure that the necessary machine and network capacity is available and correctly configured, and that Customer complies with the specified system requirements.

11.2.2 Supplier reserves the right to update Customer's solution in case a new release or version of software is available. If the use of new version or release requires upgrading of Customer's software and/or replacement of parts of equipment, Customer will cover the costs in this relation.

11.2.3 Customer is obliged at all times to assist Supplier in the implementation and delivery of Services, including (i) providing relevant existing documentation (ii) providing information to the extent Supplier may find it necessary and make necessary decisions with a time horizon which ensures the progress of the tasks (iii) under Supplier's instruction to actively participate in the process for the completion of the tasks.

11.3 Availability

11.3.1 Suppliers systems are usually available through the internet around the clock, seven days a week. Supplier and Supplier's subcontractors are entitled to take measures that affect the above availability if Supplier deems it necessary for operational reasons, technical reasons, in connection with maintenance or for security reasons. Scheduled system maintenance is notified to Customer in advance.

11.3.2 For Services for which no service level requirements are specified, the service level must be equivalent to what can be expected of a similar industry standard.

11.3.3 Customer accepts and acknowledges that access cannot be guaranteed and that Supplier cannot be held responsible for any defects and errors on the user's own internet connection or in his own equipment.

11.4 Rights

11.4.1 Customer is granted a non-exclusive right to use the Services, including software, programs, documentation and/or solutions developed by Supplier specifically for Customer. Customer may not transfer, lease or rent the right to others, and Services may only be used to carry out tasks in relation to Agreement entered into. Services may be protected by copyright.

11.4.2 Supplier reserves the right to use subcontractors, including external consultants, to fulfil its obligations.

11.4.3 Supplier has the right to terminate Services immediately if Customer or Customer's users act in violation of this Agreement.

11.4.4 Should the access for Customer be terminated, payments made in advance will not be refunded.

11.5 Termination

11.5.1 In case of termination, Customer is responsible for his own copy and export of data. Depending on the nature of the solution or Customer's wishes, Supplier can assist in exporting data. Such assistance is invoiced according to time spent at current hourly rates. Supplier cannot be held responsible for storing Customer's data after the termination of Agreement.

12. Fee, Time Consumption and Expenses

12.1 Fees are invoiced in accordance with Agreement for the agreed and performed Services. Fees may be based on time spent, number of transactions or a fixed amount for fixed tasks.

12.2 Supplier's hourly rates are differentiated according to Agreement, according to the content of the assignment and according to the qualifications of the consultants assigned.

12.3 If Customer orders consultant to provide assistance on weekends and/or holidays, the agreed hourly rate will be added 50%.

12.4 If, in connection with a fixed-price agreement, Customer orders consultant to provide assistance so that the working time for a calendar month in total exceeds the standard time for the calendar month in question (corresponding to 7.4 hours per working day * number of possible working days in the calendar month), hours are invoiced in excess of the standard time, if applicable, with the current hourly rate plus 50%.

12.5 Unless otherwise agreed, Customer pays the consultant's transport time between Customer and Supplier's nearest address.

12.6 Prices are regulated per May 1st each year based on the net price index from Denmark Statistics (upwards only) - but at least 3% per year. However, Supplier reserves the right to change rates when this is due to increased public taxes, fees or other public orders. Such amendments are implemented from the time they come into force without separate notification requirements and do not provide a basis for renegotiating the other provisions of Agreement.

12.7 Rule changes from the public sector, which will result in significant change in amount of work, will form the basis for renegotiating the price. Supplier must document an increase in the workload from the changes. The changed price will then apply from the date of the change. The same applies if there is significant extra work of a one-off nature in connection with the implementation of a rule change.

12.8 Changes in registration systems that are imposed on Supplier to fulfil Agreement and which result in a significant change in the workload will form the basis for agreeing financial compensation for extra costs. Supplier must document an increase in the workload from the changes. The changed price will then apply from the date of the change. The same applies if there is significant extra work of a one-off nature in connection with the implementation of a rule change.

12.9 Expenses are invoiced on an ongoing basis. Expenses will, for example, be transport cost according to state tariffs calculated between Customer and Supplier's nearest address, as well as expenses for parking, bridge toll, ferry, postage, and binders.

12.10 Supplier is entitled to invoice time spent in connection with Customer's need for replacement and/or update of electronic NemID / MitID (employee) signature unless it is due to Supplier's replacement of consultant.

12.11 Unless Customer receives invoices via EAN, PDF via e-mail or uses Net's supplier service (Leverandørservice), Supplier reserves the right to charge invoice fees. In addition, time spent will be invoiced if Customer requires Supplier to enter invoice into Customer's system.

12.12 Customer is obliged to provide the correct invoicing address incl. EAN number or e-mail and to notify Supplier in the event of a change. If Supplier invoices to the wrong address incl. EAN number or e-mail because Customer has not complied with its duty to provide information, Supplier re-invoices at the Customer's expense. Re-invoicing does not exempt Customer from paying on time in accordance with the original, correct invoice.

12.13 Supplier is entitled to invoice Customer for Additional Work due to Customer's late payment.

13. Payment

13.1 At the beginning of the cooperation an amount will be invoiced in advance, as a deposit equal to minimum a month's normal agreement fee. The deposit is due for immediate payment. The amount serves as security for payment and remains as a deposit until Agreement is terminated and any outstanding amounts have been paid.

13.2 Payment terms are fourteen (14) days net cash. In case of late payment, standard interest is attributed according to the provisions for late payment of commercial debt (interest).

14. Insurance

14.1 Supplier is at any time covered by professional liability insurance of NOK 20 mill. as well as crime insurance and cyber liability insurance.

15. Data Processing

15.1 Supplier must process all personal data in accordance with applicable Danish law and refrain from any processing of personal data that does not comply with the rules.

15.2 When Supplier processes data for Customer, Supplier must process Customer's personal data in accordance with Agreement entered into.

15.3 Supplier shall also process Customer's personal data in accordance with any instructions from Customer, unless the applicable law requires Supplier to act differently.

16. Confidentiality

16.1 According to their employment agreements, Supplier's consultants have a duty of confidentiality regarding matters concerning Supplier's customers. Further, Supplier's consultants have a duty of confidentiality regarding matters concerning Supplier, which Customer is requested to respect.

17. Limitation of Liability and Remedies

17.1 Supplier or its consultants cannot be held liable, financially or otherwise, because of incorrect registration in Customer's registration systems, because of Customer's breach of the law or due to other conditions.

17.2 Customer is responsible for ensuring that access to any sensitive data is not possible for Supplier's consultants. For responsibilities related to Customer's registration systems, please refer to section 10.

17.3 If Customer has matters of a special nature that Customer has not specifically informed Supplier of or if Customer has provided incorrect information, which Supplier has no basis for disputing the accuracy of, Supplier assumes no responsibility that VAT and tax liability, employee tax liability, social security contributions, and similar contributions are calculated and reported in accordance with applicable legislation and practice. The same applies to matters of a discretionary nature. In such cases, Supplier perform Services according to Customer's instructions or prior approval from Customer's auditor. It is assumed that Customer or Customer's auditor controls Customer's VAT and tax liability, employee tax liability, social security contributions etc. as well as reconciliation etc.

17.4 Customer is responsible for ensuring that access to Customer's cash or cash equivalents is not possible for Supplier's consultants. Supplier's consultants may not be awarded attorneys or authorization that may have consequences for Customer financially or otherwise in the event of errors or abuses.

17.5 The responsible person appointed by Customer must always approve transactions etc. that may have financial consequences for Customer before a transaction is executed. If Customer requires dispositions implemented where procedures regarding division of tasks and responsibilities between Supplier and Customer are not complied with, Supplier cannot be responsible for this.

17.6 Once Customer has verified and approved payment of suppliers (cf. section 6.1.4) and payroll payments (cf. section 7.3), incorrect payment cannot be imposed on Supplier.

17.7 Customer is responsible for providing codes to public authorities, which enable Supplier to perform the agreed tasks. Supplier cannot be held liable for any circumstances, such as set-offs, interest allocation, etc. that public authorities carry out towards Customer.

17.8 Supplier cannot be held responsible for or in any way be held liable for circumstances over which Supplier has no influence, e.g. theft, termination of work, etc. (cf. section 19). Similarly, Supplier cannot be held liable for accidental destruction of Customer's physical accounting material and the like, if such material is stored for Customer or be held responsible for any consequences thereof.

17.9 Supplier may be liable for a maximum amount of six (6) months of normal agreement fee unless Supplier has shown gross negligence or intent.

18. Breach of Agreement

18.1 General

18.1.1 Any claim of breach must be presented in writing without undue delay, and within six (6) months of the individual Party becoming aware of the event. If one Party does not complain in time, the right to obtain remedies is lost unless the other Party has shown gross negligence or intent.

18.1.2 In the event of material breach, Agreement may be terminated immediately by written notice.

18.2 Supplier's Breach

18.2.1 If the delivery does not take place on time, it is considered a delay. If the delivery is not in accordance with SLA, it is considered an error.

18.2.2 There is no breach if the delay or error is due to force majeure in accordance with section 19, for which Supplier is not responsible, and should not have taken into account upon signing Agreement.

18.2.3 Supplier is entitled and obliged to remedy deficiencies at his own expense. Errors can be remedied by, e.g. to correct any errors that have occurred, to redeliver or to make a further delivery so that the delivery is in accordance with Agreement. Customer's auditor or others cannot perform the work at the expense of Supplier without the Supplier's prior written approval.

18.2.4 Efforts to remedy defects and deficiencies must be initiated and carried out without undue delay as soon as the defect is discovered.

18.3 Customer's Breach

18.3.1 If Customer's obligations under Agreement are not fulfilled, it is considered a breach of Agreement.

18.3.2 Customer is considered to be in material breach of Agreement if Supplier is not given the opportunity to perform the service in an appropriate manner or Customer attempts to require Supplier to perform the service in violation of applicable laws and regulations.

18.3.3 Late Payments

a) In case Customer makes any objections to an issued invoice, such objection shall be submitted within ten (10) days from invoice date, otherwise the invoice will be considered approved. Supplier will not deal with any objection thereafter unless Customer alleges breach by following the procedures therefore.

b) If payment is not made by due date, it shall be deemed a breach of Agreement which entitles Supplier to cease work with one (1) days' notice and to offset the deposit in Supplier's outstanding balance. The same applies if Customer suspend performance or is declared bankrupt.

(c) Supplier reserves the right to invoice in advance if Customer's payment repeatedly exceed due date.

(d) It is a material breach if payment is not received within one (1) week after two (2) written reminders.

e) In the event of material breach, Supplier is entitled to withhold material.

19. Force Majeure

19.1 Supplier has entered into Agreement subject to force majeure, including but not limited to war, riots, rebellions, general strikes, fire, natural disasters, interruption or failure in energy supply, viruses, and damage to Supplier's production apparatus as well as far-reaching force majeure arising in connection with subcontractors.

19.2 There are no cases of force majeure if a subcontractor is unable to deliver, unless the subcontractor's circumstances can be attributed to section 19.1.

19.3 Supplier can only invoke force majeure if Supplier is impossible or close to impossible in fulfilment of Agreement. If applicable, Supplier has the choice between cancelling Agreement, part of Agreement, or providing the agreed Services as soon as the obstacle to normal delivery has expired. If applicable, Customer's obligations will be suspended accordingly as long as the exceptional situation lasts for Supplier.

19.4 In case of force majeure, Supplier is not responsible for any loss due to failure to deliver.

20. Damages

20.1 The Parties are liable for damages in accordance with the general rules of Danish law.

20.2 However, the Parties are solely responsible for direct losses including reasonable expenses for attorneys. The Parties are therefore in no case responsible for loss of revenue, operating loss, consequential damage or other indirect loss. Data loss is classified as indirect loss except where it is due to Supplier's handling of data. Furthermore, Supplier is not liable for any loss, the responsibility for which is waived in Agreement. Each Party's total liability under Agreement is limited to an amount equal to six (6) months of normal agreement fee prior to the claim being made. If Agreement has been active for less than six (6) months, the Party can only be liable for an amount equal to the number of active months.

20.3 Supplier also disclaims any responsibility for direct and indirect losses due to interruptions in services or communication problems, faults on Customer, errors in computer systems, electronic services or with other partners used by Customer. Supplier will at all times endeavour to remedy any errors, omissions and delays that may occur due to the above conditions.

20.4 Neither Party excludes liability for direct loss due to willful intent or gross negligence. Intent cannot be ascertained with Supplier if Supplier has arranged according to Customer's data or other material received, which Supplier has no basis for disputing the accuracy of.

20.5 Any claim for damages shall no longer apply six (6) months after the cause of action has arisen if the Party who claim to be entitled to damages has not filed a claim in this regard.

21. Dispute

21.1 Any disputes arising that cannot be resolved amicably will be settled in accordance with Danish law and may be brought by Customer or Supplier before the Det Danske Voldgiftsinstitut (The Danish Arbitration Court), which will make a final and binding decision in the case.

21.2 If, for any reason, a court of competent jurisdiction finds any provision or portion thereof unenforceable, the remainder of Agreement will remain in full force and effect.

22. Supplier Marketing

22.1 Supplier's use of Customer in its marketing requires prior acceptance. However, Supplier is authorised to include Customer in its general customer reference list.

23. Duration of Agreement

23.1 The cooperation can, unless otherwise agreed in writing, be terminated by both Parties at six (6) months' notice until the end of a month. If Customer terminates the cooperation with less than six (6) months' notice without prior mutual agreement, the greater of the following fees will be invoiced for the remaining period whether Customer makes use of Supplier's services or not calculated either based on (i) a normal month's agreement fee or based on (ii) an average of the past six (6) months invoiced time spent. If Agreement has been in effect for less than six (6) months, the average is calculated based on the current number of months invoiced time consumption.

24. Transfer

24.1 Supplier has the right to transfer its rights and obligations to another Azets Company in Denmark.

Exhibit 2
Data Processing Agreement

MADE AND ENTERED INTO BY AND BETEEWN:

Customer
(the data controller)

and

Azets Insight A/S
Lyskær 3 CD
DK-2730 Herlev
CVR 25 07 48 23
(the data processor)

each a ‘party’; together ‘the parties’

Regarding the processing of personal data in relation to eKapital Reporting Employee Share Scheme

Table of Contents

Change Log

Version	Change
1.1 - Amended by The Danish Data Protection Agency	Changes in Clauses 9.2 and 10.4 *(Corrected cross-references).*
1.2 - Amended by Azets Insight May 16th 2022	• Changed location of background and purpose • 7.2: Selection of option 2 • 7.3: Selection of option 2 - min. two (2) weeks • 9.2: Selection of supervisory authority (the Danish Data Protection Agency) • 10.2: Selection 48 hours, if possible • 11.1: Selection of option 2 • 11.2: Addition of The Danish Accounting Act • Appendix A-C adapted the processing • Appendix D adapted the data processor specifically

1. Background and Purpose

1.1 The data processor (Supplier) and the data controller (Customer) have agreed the following Standard 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.

1.2 The Clauses are based on the Danish Data Protection Agency's Standard Contractual Clauses (version 1.1 - January 2020) in accordance with Article 28 (1). 3 of Regulation 2016/679 for the processing of personal data by the data processor.

2. Preamble

2.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

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

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

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

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

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

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

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

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

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

2.11 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

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

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

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

3.3 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

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

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

5. Confidentiality

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

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

6. Security of Processing

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

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

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

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

6.3 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 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

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

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

7.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least two (2) weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

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

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

7.6 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.

7.7 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

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

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

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

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

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

8.5 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 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

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

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

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability

i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

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

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.

9.3 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1 and 9.2.

10. Notification of Personal Data Breach

10.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

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

10.3 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.

10.4 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

11.1 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.

11.2 The following 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:

a. The Danish Accounting Act.

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

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

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

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

13. The Parties' Agreement on Other Terms

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

14. Commencement and Termination

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

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

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

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

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; and **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 may only process personal data for the purposes necessary to fulfil the agreement with the data controller. Purpose must be stated here or possibly in written addenda / supplementary agreements. The data processor is entitled to include personal data in the data processor's usual backup procedure. The data processor may, to the extent not otherwise provided by the data processing agreement, use all relevant aids, including IT systems**.** ☒ eKapital Reporting Employee Share Scheme: • The purpose of the processing of personal data is that the data processor assists the data controller in preparing and performing reporting to the Danish tax authorities (SKAT) via its portal eKapital for relevant employees who are part of the data controller's employee share scheme; • As part of the assistance, the data processor accesses, registers, processes, stores and reports personal data; and • The data processor uses the application Visma Case (ESDH system) in payroll administration.
A.3. The processing may include the following types of personal data about data subjects	☒ eKapital Reporting Employee Share Scheme: The data controller's current and former employees. General Personal Data: • employee number; • employment and resignation date; • name and address; • contact information, including phone, e-mail, title, department, address; • payroll information including information on employee share scheme and working hours; and • pension and tax information. Confidential Personal Data: • CPR-number. ☒ The Application Visma Case (ESDH system): The data controller's current and former employees. General, Sensitive, and Confidential Personal Data: • Cf. eKapital reporting of employee share scheme.
A.4. Processing includes the following categories of data subject	See the overview in A.3.
A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration	The data processing of personal data follows the duration specified in any active Service agreement, as well as the data controllers' instructions in Regulations 11.1 and 11.2.

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	ADRESS	DESCRIPTION OF PROCESSING
☒	Azets Insight SRL	VAT RO24813426 Org. J32/1906/2008	Str. Nicolaus Olahus, nr. 5 Et. 9-10 550370 Sibiu, Romania	Administrative assistance
☒	Azets Software AB	Org. no. 559273-6937	Ekensbergvägen 113 SE-171 41 Solna	Hosting, development and maintenance of Azets Cozone Portal/Activity/ Drive/Employee
☒	Visma IMS A/S	CVR no. 25 86 20 15	Søren Frichs Vej 440 DK-8230 Åbyhøj	Hosting, development and maintenance of the ESDH system Visma Case

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.

B.2. Prior Notice for the Authorisation of Sub-processors

The data processor may generally change or introduce sub-processors provided that the processing is within the EU/EEA, by giving notice as set forth in Clause 7.3.

Appendix C Instruction Pertaining to the Use of Personal Data

C.1. The subject of/instruction for the processing	The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following: See Appendix A item A.1 / A.2.
C.2. Security of processing. The level of security must reflect: (includes all systems unless specified)	The processing of data includes personal data, as mentioned in Appendix A item A.3 / A.4 and which may be - but not necessarily - covered by Article 9 of the Data Protection Regulation on "special categories of personal data", for which reason a "high" security level must be established. The data controller is entitled and obliged to make decisions about what technical and organisational security measures must be implemented to establish the necessary (and agreed) level of security. The data processor guarantees to the data controller that the data processor will implement the appropriate technical and organisational security measures in such a way that the data processor's processing of personal data meets the requirements of the personal data law regulation in force at any given time. The data processor shall however - in any case and as a minimum - implement the measures described in item C.2.1 - C.2.15, which have been agreed with the data controller.
C.2.1 Pseudonymization and encryption of personal information	The data processor is obliged to implement and maintain appropriate technical and organisational security measures to ensure that personal information is pseudonymised, where applicable to services. The data processor is obliged to implement and maintain appropriate technical and organisational security measures that ensure that the personal data is encrypted or otherwise protected against e.g. unauthorized access and / or tampering, in particular in connection with transmission via open networks and / or external communication links. The level of encryption must be appropriate to effectively prevent unauthorized access to personal information. See item C.2.7.
C.2.2 Ensuring the confidentiality, integrity, availability and robustness of processing systems and services	The confidentiality of the data processor's employees is specified in item C.2.6. Technical security of the data processor: • Virus definitions are updated daily; • Local firewall on PC's and servers is enabled; • Network is protected by firewall; • Ongoing internal and external vulnerability scans to ensure optimal configuration; • Employees and external consultants have external access to networks via encrypted connections with MFA; • Data on all PCs is encrypted; • Complex passwords are used; • Exchange of personal data with data controller etc. happens via encrypted connections, for example SFTP or web portals; and • Continuous backup of data.

	Organisational security of the data processor: • Authorization procedures, access rights, logging, etc. according to the data processor's internal IT procedures; and • Employees and external consultants receive security training and adequate instructions in and guidelines for the processing of personal data and IT security.
C.2.3 Recovery of personal data and operation	The data processor is obliged to implement and maintain appropriate technical and organisational security measures that ensure timely restoration of access to the personal data in the event of physical incidents (e.g. power outages, fire, flood, lightning, etc.) and / or technical incidents (system crashes, etc.), including in the form of contingency plans, procedures, etc. The data processor is obliged to carry out and maintain documented emergency preparedness procedures that ensure the re-establishment of services without undue delay in the event of operational interruptions.
C.2.4 Procedure for regular testing, assessment and evaluation of the effectiveness of technical and organisational security measures to ensure processing safety (includes all systems unless specified)	The data controller is obliged to implement and maintain appropriate technical and organisational security measures for regular testing, assessment and evaluation of the effectiveness of the technical and organisational security measures to ensure processing security. The data processor carries out annual inspections of subcontractors by reviewing data processor agreements for the individual subcontractors as well as a risk assessment. Any issues are followed up (see item C.8). ☒ The Application Azets Cozone (Data Exchange): • The sub-processor conducts ongoing vulnerability scans of infrastructure and annual penetration testing of application. ☒ The Application Visma Case (ESDH System): • The sub-processor conducts ongoing vulnerability scans of infrastructure and annual penetration testing of application.
C.2.5 Staff access to personal data	The data processor ensures through formal approval processes as well as recurring control of accesses that only persons with a documented work-related need have access to personal data. The data processor must, without undue delay, cancel authorizations (including accesses) for users who no longer have a work-related need for authorization.
C.2.6 Confidentiality	All employees of the data processor and external consultants are subject to a contractual duty of confidentiality with regard to everything the employee experiences during his work for the data processor about all business and confidential information concerning parties with whom the data processor is connected. The duty of confidentiality also applies after the termination of the employment relationship.
C.2.7 Data protection during transmission and at rest (includes all systems unless specified)	The data processor is obliged to implement and maintain appropriate technical and organisational security measures that ensure that personal data is protected against, among other things: unauthorized access and / or tampering.

	Encryption of the transport layer must at all times meet the Danish Data Protection Agency's minimum requirements. ☒ The Application Azets Cozone (Data Exchange): • External file delivery to and from solution takes place via SFTP or FTPS connection; • All communication to and from the solution is encrypted, either via web services, HTTPS requests via the web solution or communication to / from the App; and • The solution is encrypted during storage and is accessed in encrypted form via web and / or App (iOS and Android). ☒ The Application Visma Case (ESDH System): • The solution is accessed in encrypted form via web; and • All communication to and from the solution is encrypted, either via HTTPS requests via the web solution or communication via API.

C.2.8 Physical security of locations where personal data is processed
 	
(includes all systems unless specified)
	The data processor is obliged to implement and maintain appropriate physical, technical and organisational measures that secure the physical locations where personal data is processed against, among other things, unauthorized access and / or tampering with data.
	
	Physical access security has been established so that only authorized persons can gain physical access to premises and data centres in which personal data are stored and processed.
	
	☒ The Application Azets Cozone (Data Exchange):
	
	• The solution is operated from Amazon Web services with the following global certifications around e.g. access security:
	  ○ AWS ISO/IEC 27001:2013;
	  ○ AWS ISO/IEC 27017:2015;
	  ○ AWS ISO/IEC 27018:2019;
	  ○ AWS ISO/IEC 9001:2015;
	  ○ AWS SOC 1 Report;
	  ○ AWS SOC 2 Security, Availability & Confidentiality;
	  ○ AWS SOC 2 Privacy Type I; and
	  ○ AWS SOC 3 Security, Availability & Confidentiality

C.2.9 Backup	Backup of systems, configuration files and data must take place so that relevant data can be re-established. The backup copies are stored in such a way that they are not accidentally or illegally (for example by fire, flood, accident, theft or the like) destroyed, lost, degraded, come to the knowledge of unauthorized persons, misused or otherwise treated in violation of the rules and regulations in force at any time for the processing of personal data. Including amongst others: • The same guidelines apply to backup copies as to any other processing of personal data under Agreement and this data processing agreement; • Backups are stored geographically separate from the primary data centre; and • The data processor continuously checks that backups are readable.
C.2.10 Password policy and control of rejected access attempts	The data processor is obliged to implement and maintain appropriate technical and organisational security measures that ensure that passwords are of appropriate length and complexity to prevent them from being guessed. Passwords must be changed regularly and mandatorily several times a year to prevent them from being used by unauthorized persons to access the data processor's systems or data.

	Passwords must be unique to the individual employee and external consultant. The data processor is obliged to register rejected access attempts and block further attempts after a fixed number of consecutive rejected access attempts.
C.2.11 Home workplaces	The data processor is obliged to implement and maintain appropriate technical and organisational measures that ensure that personal data is protected against, among other things, unauthorized access and / or tampering when accessed from home and remote workplaces, and that access to personal data from home and remote workstations use encryption of communication connections as well as authentication of persons gaining access. All computers are encrypted and password protected. Access to the data processor's systems is via VPN connection with MFA. Any print is minimized as much as possible and must be shredded after use. Employees and external consultants must regularly undergo mandatory awareness training in accordance with item C.2.12.
C.2.12 Awareness training	The data processor is obliged to ensure that employees and external consultants regularly (and at least annually) undergo mandatory training on IT security and data protection.
C.2.13 Change management	The data controller is required to have formal change management procedures in place to ensure that any change is duly authorized, tested and approved before implementation.
C.2.14 Logging	The data processor is obliged to implement and maintain appropriate technical and organisational measures that ensure logging so that incidents can be tracked. Logs must contain timestamps and, where applicable, user ID, terminal ID and network addresses. As a minimum, the following security incidents must be logged: • rejected access attempts; and • successful and rejected authentication attempts due to account lockout triggered by access control system. Access to personal data must be logged to such an extent that the log data can be used to prevent unauthorized access to personal data. Where relevant, access to personal data must be logged, including what data is accessed, the processing of data as well as time and identity information. Log is stored for a maximum of thirteen (13) months. In case of incidents, storage can be extended. The backup archive is stored for a maximum of six (6) years (cf. Appendix D regarding Regulations 11.1 and 11.2). During the same period, the data processor is entitled to have the personal data included in the data processor's usual backup procedure.
C.2.15 Data protection advisor and IT security personnel	The data controller is required to have appointed one or more data protection advisers, as described in the Data Protection Regulation. The data processor is required to have dedicated resources to maintain the data processor's IT security.

C.3. Assistance to the data controller	The data controller shall, to the extent necessary and reasonable, assist the data controller in fulfilling his / her obligations when processing personal data covered by the provisions of paragraphs 9 and 10 by implementing such technical and organisational measures as may contribute to the data controller's ability to respond to requests on the exercise of the rights of data subjects.
C.4. Storage period/erasure procedures	Personal data is stored for a maximum of six (6) years in accordance with the requirements of the Accounting Act (cf. Appendix D regarding Clauses 11.1 and 11.2). Upon termination of Services relating to the processing of personal data, the data processor shall either delete or return the personal data in accordance with Clause 11.1, unless the data controller - after signing these provisions - has changed the original choice. Such changes must be documented and stored in writing, including electronically, in connection with the Clauses.
C.5. Processing location	The processing of the personal data covered by the Clauses may not take place without the prior written consent of the data controller at locations other than the following, in addition to the sub-processors listed in Appendix B: • The data processor's locations in Denmark at all times; and • Home and Remote Workstations (Data Processor's Employees and External Consultants).
C.6. Instruction on the transfer of personal data to third countries	If the data controller does not in these Clauses or subsequently provide a documented instruction regarding the transfer of personal data to a third country, the data processor is not entitled to make such transfers within the framework of these Clauses.
C.6.1 Cloud provider and data transfer mechanism	If the data processor uses a cloud provider in connection with the provision of Services (cf. Appendix B), only data centres within the EU / EEA may be used.
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 has access to carry out inspections, including physical inspections, with the locations from which the data processor processes personal data, including physical locations and systems used for or in connection with the processing. Such inspections may be carried out when the data controller deems it necessary. However, this does not apply to the data processor's home workstations. The data controller must give the data controller at least thirty (30) days notice before inspection. If the data controller or a representative of the data controller carries out an inspection at the data processor, he or she must present a valid image identification. The person's identity and purpose must be confirmed by the data controller's contact person before he or she has access to confidential information. The data controller or the representative of the data controller must comply with all security requirements that may apply to the location. The data controller's expenses in connection with a physical inspection are borne by the data controller. The data processor is obliged to

	allocate for remuneration the resources (mainly the time) necessary for the data controller to carry out his inspection.

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 processor may carry out an annual physical inspection of the sites from which sub-processors process personal data, including physical sites and systems used for or in connection with the processing, in order to determine the sub-processor's compliance with the Data Protection Regulation in other EU law or the national law of the Member States and these Clauses.
	
	In addition to the annual inspection, the data processor shall carry out an inspection with the sub-data processor when the data processor deems it necessary.
	
	Based on the results of the monitoring, the data controller is entitled to request, at his own expense and risk, the implementation of additional measures to ensure compliance with the Data Protection Regulation, data protection provisions of other EU law or Member States' national law and these Clauses.
	
	The data controller may challenge the framework for and / or the method of the inspection and in such cases may, at his own expense and risk, request the conduct of a new inspection under another framework and / or using another method.
	
	The parties agree that the following type of certificate may be applied in accordance with these Clauses in the following areas of sub-processor:
	
	• BPO payroll processing on the application EPOS Payroll: ISAE 3402 Type II;
	• BPO payroll processing on the application Zenegy Payroll: ISAE 3402 Type II;
	• The application Azets Cozone (data exchange): None
	• The application EPOS Payroll: None;
	• The application EPOS HR: None;
	• The application EPOS Recruitment: None;
	• The application EPOS Management: None;
	• The application Workcyclus (Workplace Assessment): None;
	• The application zExpense (Expenses): ISAE 3000 Type I
	• E-Boks delivery of payslips:
	  ○ ISAE 3000 Type I and II
	  ○ ISO27001:2013 Compliance;
	• The application Visma Case (ESDH system):
	  ○ ISAE 3000 Type I
	  ○ ISAE 3402 Type II
	  ○ ISO27001 Compliance
	
	The above certificates are sent on request without charge and unnecessary delay to the data controller for information.
	
	The certificates are confidential and may not be shared with unautho-rized persons.

Appendix D The Parties' Terms of Agreement on Other Subjects

In addition to the Clauses, the parties have agreed the following:

Regarding Clause 7.6:

The parties have deviated from Clause 7.6, which does not apply to the agreement.

Regarding Clause 11.1 and 11.2:

The data processor keeps bookkeeping and accounting material in a secure manner for five (5) years from the end of the financial year to which the material relates, unless the data controller confirms in writing to take over responsibility for this.

Regarding Clause 13.1:

Liability:

The parties' liability under the Clauses shall be subject to the same limitation of liability as agreed between the parties in the service agreement(s) under which the personal data is processed.

The data controller shall be liable for the damage caused by processing which infringes the data protection legislation. The data processor shall only be liable for direct and documented damages caused by processing where the data processor has breached the Clauses and/or data protection legislation specifically directed to the data processor's obligations.

For the avoidance of doubt, the parties agree and acknowledge that each party shall be liable for and held accountable to pay all administrative fines and damage caused to the data subject, which a party has been imposed to pay in accordance with the data protection legislation.