Data Processing Agreement

between

[Name]

CVR-no. [Company registration number]

[Address]

[Postcode and town]

(the "Data Controller")

and

Pramo ApS

CVR-no. 34 69 00 81

Bagsværd Hovedgade 141, 1st right

2880 Bagsværd

(the "Data Processor")

1 Contents

2 Background to the Data Processing Agreement

1. This Data Processing Agreement (the "Agreement") lays down the rights and obligations which apply when the Data Processor performs the processing of personal data on behalf of the Data Controller.

2. The Agreement is designed with a view to the Parties' compliance with Article 28(3) of the *Regulation (EU) 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)*, which provides specific requirements for the contents of a data processing agreement.

3. The Data Processor's processing of personal data shall be with a view to fulfilling the Cooperation Agreement of [date] (the "Main Agreement") concluded between the Parties.

4. The Data Processing Agreement and the Main Agreement are interdependent and cannot be terminated separately. The Data Processing Agreement may, without terminating the Main Agreement, be replaced by another valid data processing agreement.

5. This Data Processing Agreement has precedence in relation to any corresponding provisions in other agreements between the Parties, including those found in the Main Agreement.

6. This Agreement has four appendices. These appendices operate as an integrated component of the Data Processing Agreement.

7. Appendix A of the Data Processing Agreement contains detailed information about the processing, including on the intent and nature of the processing, the type of personal data, the categories of data subjects and duration of the processing.

8. Appendix B of the Data Processing Agreement contains the Data Controller's conditions for the use of subcontracting data processors by the Data Processor and a list of any subcontracting data processors that have been approved by the Data Controller.

9. Appendix C of the Data Processing Agreement contains more detailed instructions about the nature of the processing which the Data Processor is expected to perform on behalf of the Data Controller (subject of the processing), the minimum security measures that must be observed and the Data Processor and any subcontracting data processors are monitored.

10. The Data Processing Agreement and its appurtenant appendices shall be retained in writing, hereunder in electronic form, by both Parties.

11. This Data Processing Agreement does not free the Data Processor from obligations which are directly imposed on the Data Processor pursuant to the Data Protection Regulation or any other legislation.

3 The Data Controller's rights and obligations

1. As a rule of thumb, the Data Controller has a universal (including to each data subject) responsibility to ensure that the processing of personal data occurs within the framework of the Data Protection Regulation and the Danish Act on the Protection of Personal Data.

2. The Data Controller has therefore both rights and obligations to make decisions about the permitted purposes of the processing and which aids may be used to assure its performance.

3. The Data Controller is (inter alia) responsible for assuring that there is a legal basis for the processing that the Data Processor is instructed to perform.

4 The Data Processor shall act in accordance with instructions

1. The Data Processor may only process personal data after having received documented instructions from the Data Controller, unless it is required to do so by EU law or national law in the Member States, to which the Data Processor is subject. In such case, the Data Processor shall inform the Data Controller of such legal requirements before processing, unless that legislation prohibits such reporting on important grounds of public interest, cf. Article 28(3)(a).

2. The Data Processor shall immediately notify the Data Controller if the Data Processor believes that an instruction is in conflict with the Data Protection Regulation or data protection provisions of other EU legislation or the national law of the Member States.

5 Confidentiality

1. The Data Processor shall ensure that only those who are currently authorised for that purpose, are able to gain access to the personal data that is processed on behalf of the Data Controller. Access to the data must immediately be removed if the authorisation expires or is removed.

2. Only those persons for whom it is necessary to have access to the personal data in order to fulfil the Data Processor's obligations towards the Data Controller may be granted such authorisation.

3. The Data Processor shall ensure that the persons who are authorised to process personal data on behalf of the Data Controller, have accepted a duty of confidentiality or are subject to an appropriate statutory duty of secrecy.

4. At the request of the Data Controller, the Data Processor must be able to demonstrate that any relevant employees are subject to the aforementioned duty of secrecy. Recomment that the contract between employee and employer, is filed with information about secrecy.

6 Security of processing

1. The Data Processor shall implement any and all measures that may be required in accordance with Article 32 of the Data Protection Regulation, which, inter alia, specifies that, taking into account the current level, costs of implementation and the nature, scope, context and purpose of the specific processing and the risks of varying likelihood and severity to the rights and freedoms of natural persons, appropriate technical and organisational measures must be implemented in order to ensure a level of security that is appropriate to these risks. Pramo has security protection of software and processing within Pramo and from the IT provider.

2. The aforementioned obligation requires that the Data Processor shall perform a risk assessment and then implement measures to accommodate any identified risks. This may, inter alia and depending on what is appropriate, include the following measures:

    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 of and access to the personal data in a timely manner in the event of a physical or technical incident
    d. A procedure for regular testing, assessing and evaluating the effectiveness of the technical and organisational measures to ensure security of processing

3. Within the context of the above, the Data Processor must in all cases and by way of minimum implement the level of security and the measures which are specified in further detail in Appendix C to the present Agreement.

4. The Parties' regulation/agreement for remuneration or the like in connection with the Data Controller's or Data Processor's subsequent demands for the implementation of additional security measures will be apparent from the Parties' Main Agreement or in Appendix D to the present Agreement.

7 The use of subcontracting data processors

1. The Data Processor shall fulfil the conditions referred to in Article 28(2) and (4) of the Data Protection Regulation if it is to be permitted to employ another data processor (subcontracting data processor).

2. The Data Processor may therefore not use another data processor (subcontracting data processor) for the fulfilment of the Data Processing Agreement without prior specific or general written approval by the Data Controller.

3. In the case of general written approval, the Data Processor shall inform the Data Controller of any proposed changes concerning the addition or replacement of other data processors and thereby provide the Data Controller with the opportunity to contest such changes.

4. The Data Controller's detailed conditions for the Data Processor's use of any subcontracting data processor are outlined in Appendix B of the present Agreement.

5. Any approval by the Data Controller of specific subcontracting data processors shall be listed in Appendix B of the present Agreement.

6. Once the Data Processor has gained the Data Controller's approval to use a subcontracting data processor, the Data Processor shall ensure that the subcontracting data processor is subject to the same data protection requirements as those laid down in this Data Processing Agreement, in the form of a binding contract or other legal document pursuant to EU law or national law in the Member States, which specifically stipulates the required guarantees that the subcontracting data processor will implement the appropriate technical and organisational measures in such a way that the processing is compliant with the requirements of the Data Protection Regulation.

   The Data Processor is thus responsible (through the conclusion of a subcontracting data processor agreement) for imposing on any subcontracting data processor by way of minimum the obligations to which the Data Processor is itself subject, pursuant to data protection regulations and this Data Processing Agreement with its appendices.

7. If so requested by the Data Controller, a copy of the subcontracting data processor agreement and any subsequent amendments thereto shall be sent to the Data Controller, allowing the Data Controller to ensure that a valid agreement exists between the Data Processor and the subcontracting data processor. Any commercial conditions, such as price information which do not affect the legal data protection content of the subcontracting data processor agreement shall not be sent to the Data Controller.

8. If the subcontracting data processor fails to fulfil its data protection obligations, the Data Processor shall be fully liable to the Data Controller for the fulfilment of the subcontracting data processor's obligations.

8 The transfer of data to third countries or international organisations

1. The Data Processor may only process personal data in accordance with documented instructions from the Data Controller, including as regards the transfer (handover, disclosure

and internal application) of personal data to third countries or international organisations, unless it is required to do so under EU law or national law in the Member States to which the Data Processor is subject. In this case, the Data Processor shall inform the Data Controller of such legal requirements before processing, unless relevant legislation prohibits such reporting on important grounds of public interest, cf. Article 28(3)(a).

2. Without the Data Controller's instruction or approval, the Data Processor may not within the framework of the Data Processing Agreement inter alia;

    a. disclose personal data to a data controller in a third country or an international organisation,
    b. allow the processing of personal data to be performed by a subcontracting data processor in a third country
    c. allow the data to be processed at another unit owned by the Data Processor that is located in a third country.

3. Any transfer of personal data to a third country that has been instructed or approved by the Data Controller is stated in Appendix C of this Agreement.

9 Assistance to the Data Controller

1. Taking into account the nature of the processing and by means of appropriate technical and organisational measures, the Data Processor shall as far as possible assist the Data Controller in the Data Controller's fulfilment of its obligation to respond to requests for the exercise of the rights of data subjects as laid down in Chapter 3 of the Data Protection Regulation.

    This implies that the Data Processor shall as far as possible assist the Data Controller in connection with the Data Controller's assurance of compliance with:

    a. its obligation to provide information when collecting personal data from the data subject
    b. its obligation to provide information if personal data is not collected from the data subject
    c. the data subject's right to insight
    d. the right to have information corrected
    e. the right to have information deleted ("the right to be forgotten")
    f. the right to limitation of processing
    g. the obligation to provide information in connection with the correction or deletion of personal data limitation of processing
    h. the right to data portability
    i. the right to object

j. the right to object to the result of automatised individual decisions, including profiling

2. The Data Processor shall assist the Data Controller in its assurance of compliance with the Data Controller's obligations pursuant to Articles 32-36 of the Data Protection Regulation, taking into account the nature of the processing and the information that is available to the Data Processor, cf. Article 28(3)(f).

   This implies that the Data Processor shall, taking into account the nature of the processing, assist the Data Controller in connection with the Data Controller's assurance of compliance with:

   a. the obligation to implement appropriate technical and organisational measures to ensure a level of security that is appropriate to the risks associated with the processing
   b. the obligation to give notification in the event of any breach of personal data security to the supervisory authority (The Danish Data Protection Agency) without undue delay and if possible within 72 hours after the Data Controller has become aware of the breach, unless it is unlikely that the personal data security breach involves a risk to the rights or freedoms of natural persons.
   c. the obligation to inform data subject(s) without undue delay of any breach of personal data security, when such a breach is likely to involve a high risk to the rights and freedoms of natural persons
   d. the obligation to perform an impact assessment on data protection, if a type of processing is likely to represent a high risk to the rights and freedoms of natural persons
   e. the obligation to consult the supervisory authority (The Danish Data Protection Agency) before processing, if a data protection impact assessment shows that the processing will lead to high risk due to the absence of measures implemented by the Data Controller to reduce any such risk

3. Any regulation/agreement between the Parties concerning remuneration or similar in connection with the Data Processor's assistance to the Data Controller will appear in the Parties' "main agreement" or in Appendix D to this Agreement.

10 Notification of personal data security breach

1. The Data Processor shall inform the Data Controller without undue delay after becoming aware that there has been a breach of personal data security at the Data Processor, or any subcontracting data processor.

   When possible, the Data Processor's notification to the Data Controller must be within 24 hours after the former has become aware of the breach, so that the Data Controller is able

to comply with its obligation to give notification of the breach to the supervisory authority within 72 hours.

2. In accordance with clause 10.2.b of the present Agreement, the Data Processor shall, taking into account the nature of the processing and the information that is available to the Data Processor, assist the Data Controller towards its notification of the breach to the supervisory authority.

   This may mean that the Data Processor shall, inter alia, assist in the production of the following information which, pursuant to Article 33(3) of the Data Protection Regulation, must be stated in the Data Controller's notification to the supervisory authority:

   a. The nature of the personal data security breach, including (if possible) the categories and the approximate number of affected data subjects and their categories and the approximate number of affected registrations of personal data
   b. The probable consequences of the personal data security breach
   c. The measures that have been taken or that have been proposed to manage the personal data security breach including, if appropriate, measures to restrict its possible harmful effects

11 Deletion and return of data

1. Upon termination of the services relating to the processing, the Data Processor is duty bound, at the Data Controller's discretion, to delete or to return all personal data to the Data Controller and to delete existing copies, unless EU law or national law prescribes the storage of personal data.

12 Supervision and auditing

1. The Data Processor shall make all information available which is required in order to demonstrate the Data Processor's compliance with Article 28 of the Data Protection Regulation and the present Agreement to the Data Controller and enable and contribute to any revisions, including inspections performed by the Data Controller or another auditor who is authorised by the Data Controller.

2. The details of the procedure for the Data Controller's supervisory inspection of the Data Processor is outlined in Appendix C of the present Agreement.

3. The Data Controller's supervision of any subcontracting data processors shall normally be via the Data Processor. The detailed procedure for this is outlined in Appendix C of the present Agreement.

4. The Data Processor is duty bound to grant access to the Data Processor's physical facilities against presentation of appropriate credentials to the currently legally determined authorities who have a legal basis to gain access to the Data Controller or Data Processor's facilities, or representatives acting on the behalf of those authorities.

13 The Parties' agreements on other conditions

1. A possible (special) regulation of the consequences of the Parties' breach of the Data Processing Agreement will be provided for in the Parties' Main Agreement.

2. A possible regulation of other relationships between the Parties will be stated in the Main Agreement.

14 Entry into force and expiry/termination

1. This Agreement enters into force upon its signature by both Parties.

2. Both Parties may require that the present Agreement be renegotiated, if changes in legislation or deficiencies within the Agreement give cause to do so.

3. The Parties' regulation/agreements on remuneration, conditions or similar in connection with any amendments to the present Agreement will be stated in the Parties' Nain Agreement.

4. This Data Processing Agreement may be terminated pursuant to the notice of termination as laid down in the Main Agreement.

5. The Agreement shall endure for as long as the processing persists. Regardless of the termination of the "main agreement" and/or the Data Processing Agreement, the Data Processing Agreement shall endure until the processing has ceased and any data has been deleted at the Data Processor's premises and those of any subcontracting data processors.

6. Signatures

Representing the Data Controller		Representing the Data Processor	
Name:		Name:	Dorthe Nørregaard
Position:		Position:	CEO
Date:		Date:	25. maj 2018
Signature:		Signature:	

15 Contact persons/points of contact at the Data Controller and the Data Processor

1. The Parties may contact each other via the following contacts/points of contact:

2. The Parties are required to inform each other of any changes regarding their contact person/point of contact on an ongoing basis.

Name:		Name:	Dorthe Nørregaard
Position:		Position:	CEO
Telephone number:		Telephone number:	+45 23900199
Email:		Email:	Dorthe@Pramo.dk

Bilag A Information about the processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller:

- [The purpose of the processing is to do payroll on behalf of the Data Controller].

The Data Processor's processing of personal data on behalf of the Data Controller primarily concerns (the nature of the processing):

- processing information on employees and independent contractors of the Data Controller in order to pay out salary and other entitlements, withhold pension, tax and other contributions and pay/report pension etc. to the pension company and the tax authority and other relevant authorities.

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

- Name, email address, telephone number, address, social security number (CPR), CVR number, payment details, working hours, salary, pension contributions, benefit details, bonus, overtime, holiday allowance, maternity/paternity leave, periods of sickness, holiday periods, tax withholding rate and tax deduction.

The processing shall include the following categories of data subjects:

- Employees and independent contractors of the Data Controller.

The Data Processor's processing of personal data on behalf of the Data Controller may commence after the present Agreement has entered into force. The processing has the following duration:

- Processing is not time limited and shall endure until the Main Agreement is terminated by one of the Parties.

Bilag B Conditions for the Data Processors' use of subcontracting data processors and list of approved subcontracting data processors

B.1 Conditions for the Data Processor's use of any subcontracting data processors

The Data Processor has the Data Controller's general approval to make use of subcontracting data processors. The Data Processor must, however, inform the Data Controller of any proposed changes concerning the addition or replacement of other data processors, thereby giving the Data Controller the opportunity to contest such changes. Such notification shall be submitted to the Data Controller at least 1 month before the use or the amendment shall enter into force. If the Data Controller has objections to these changes, the Data Controller shall give notice in this regard to the Data Processor 2 weeks after receipt of the notification. The Data Controller may only raise objections, if the Data Controller has reasonable, specific cause to do so.

B.2 Approved subcontracting data processors

Upon the entry into force of the Data Processing Agreement, the Data Controller has authorised the use of the following subcontracting data processors:

Name	CVR no.	Address	Description of the processing
[Addvission]	[25189620	Kantatevej 26B 2730 Herlev	Responsible for the host of systems. Backup.
PA Kompens		Singelgatan 7 212 28 Malmø	WeB-office, file sharing office on internet

Upon the entry into force of the Data Processing Agreement, the Data Controller has specifically approved the use of the aforementioned subcontracting data processors for precisely the processing which has been described next to the Party's name. The Data Processor may not, without the Data Controller's specific and written approval, use the individual subcontracting data processor for any "other" processing that the agreed, or allow another subcontracting data processor to perform the described processing.

Bilag C Instructions concerning the processing of personal data

C.1 The subject of the processing/ Instructions

The Data Processor's processing of personal data on behalf of the Data Controller shall be the performance by the Data Processor as set out in Section of the Main Agreement. The IT provider do not have any kind of personal data, The Company is Pramo IT department, to be shure that there is Backup and systems always is in operation.

C.2 Security of processing

The level of security must reflect:

The Data Processor is entitled and required to make decisions about the technical and organisational security measures that need to be applied in order to establish the necessary level of security with respect to the data.

The Data Processor shall however, in all cases and by way of minimum, implement the following measures as agreed with the Data Controller (on the basis of the risk assessment performed by the Data Controller):

Describe any requirements relating encryption of personal data. When files are sent by E-mail, they are protected by a password that is not in the E-mail, but by agreement only know to Pramo and to the reciver.

Describe any requirements relating to the ability to ensure continuous confidentiality, integrity, availability and resilience of processing systems and services. By regular meeting within every quarter of the year, Pramo ensures the rules of GDPR protection, and that only nessacary data will be sent, and always using an agreed password.

Describe any requirements relating to the ability to respond in a timely manner to restore the availability of and access to the personal data in the event of a physical or technical incident data available in Pramo´s IT system, are backed-up by the IT-provider in more than one database, and can always be restored.

Describe any requirements concerning procedures for periodic testing, assessing and evaluating the effectiveness of the technical and organisational measures that have been implemented to ensure security of processing. All technical processing undergoes an annual audit from PWC.

Describe any requirements relating to access to data via the Internet, All access to internet-based data is only possible by using password protection.

Describe any requirements relating to the protection of data, where it is to be transmitted. For data transmitted by e-mail, see the description before. For data transmitted to an IT provider it is passeword – protected whether it is upload or download

Describe any requirements relating to the protection of data, where it is to be stored. Data stored electronically are always password protected. Data stored on paper is stored in a locked facility, from 2017 only electronical storage is used.

Describe any requirements relating to physical security of locations where personal data is processed. Physical data is stored in a locked facility, that only Pramo has access to. And the whole area is protected by a security alarm.

Describe any requirements relating to the use of home/remote. Working from Home/remote places is only possible by access with password. The employees are instructed to always use screen-password protection when they are away from the workplace.

Describe any requirements concerning logging, There is no special requirements for logging data.

C.3 Storage period/deletion routine

Enter any relevant storage period/deletion routine for the Data Processor: Variable data for employees who are still employees are saved for 5 years.

Contracts for employees will be stored forever, upon termination, the contract will be canceled after 5 years.

C.4 Processing location

The processing of the personal data that is encompassed by the present Agreement may not be performed at other locations than the following, without prior written authorisation by the Data Controller:

- To process the entire process for a payroll, there will be data that must be forwarded to pensioncompany, tax etc. In case, only the relevant data will be sent, in order for the process.
- There will be several pension companies where Pramo will send the relevant informations.

C.5 Instruction or approval of the transfer of personal data to third countries

If the Data Controller has not in this section, or in a subsequent written communication, stated an instruction or approval for the transfer of personal data to a third country, the Data Processor shall not perform any such transfer within the framework of the Data Processing Agreement.

C.6 Detailed procedures for the Data Controller's supervision/inspection of the processing that is performed at the Data Processor's premises

The Data Processor must once a year and at the Data Controller's expense obtain an auditors' statement from an independent third party, regarding the Data Processor's compliance with this Data Processing Agreement and its appendices.

The auditors' statement shall be sent to the Data Controller as soon as possible after it has been obtained, for information purposes.

The Data Controller or a representative for the Data Controller shall also be granted access to perform inspections, including physical inspections at Data Processor's premises if the Data Controller deems that this is necessary.

C.7 Detailed procedures for the inspection of processing which is performed by any subcontracting data processors

Once a year, the Data Processor shall at the Data Controller's expense obtain an auditors' statement from an independent third party regarding the subcontracting data processor's compliance with the present Data Processing Agreement and its appendices.

The auditors' statement shall be sent to the Data Controller as soon as possible after it has been obtained, for information purposes.

The Data Processor or a representative of the Data Processor shall also have access to perform supervisory inspections, including physical inspections at the subcontracting data processor's premises when the Data Processor (or the Data Controller) deems it necessary.

Documentation in relation to the supervisory inspection shall be sent as soon as possible to the Data Controller, for information purposes."