DATA PROCESSOR AGREEMENT

BETWEEN

The Data Controller:

<Company>

Org. nr. 927810921

AND

The Data Processor:

Capana ApS

CVR 10127521

Østre Alle 6, 1 sal

DK-9530, Støvring

capana

Data Processor Agreement

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Anders Frost		2023.01.01	2023-01-01	Commercial-in-confidence

CONTENTS

capana

Data Processor Agreement

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Anders Frost		2023.01.01	2023-01-01	Commercial-in-confidence

1. BACKGROUND FOR THE DATA PROCESSOR AGREEMENT

This agreement sets out the rights and obligations that apply when the Data Processor handles personal data, on behalf of the Data Controller.

The agreement is designed for the parties to comply with Article 28 (1). 3 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals, with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (Data Protection Regulation), which sets specific requirements for the content of a Data Processing Agreement.

The Data Processor Agreement and the “Main Agreement” are interdependent and cannot be terminated separately. However, the Data Processor Agreement may – without terminating the “Main Agreement” – be replaced by another valid Data Processor Agreement. This Data Processor Agreement takes precedence over any similar provisions in the other agreements between the parties, including the “Main Agreement”. For this agreement are four appendices. The attachments act as an integral part of the Data Processor Agreement.

The Data Processor Agreement Appendix A contains details of the treatment, including the purpose and nature of the treatment, the type of personal data, the categories of registered and duration of treatment.

The Data Processor Agreement Appendix B contains the Data Controller´s conditions for the Data Processor to make use of any Sub Data Processors, as well as a list of Sup Data Processors approved by the Data Controller.

The Data Processor Agreement Appendix C contains a detailed instruction on the processing by the Data Processor on behalf of the Data Controller (the subject of the processing), which minimum security measures should be observed, and how the Data Processor and any Sub Data Processor are supervised.

The Data Processor Agreement Appendix D contains the parties’ possible regulation of matters not otherwise stated in the Data Processor Agreement or the parties “Main Agreement”. The Data Processor Agreement and its supporting documents are stored in writing, including electronically by both parties.

This Data Processor Agreement does not release the Data Processor for any obligations that are directly imposed on the Data Processor under the Data Protection Regulation or any other law.

2. DATA RESPONSIBILITIES AND RIGHTS

The Data Controller is responsible for the processing of personal data within the scope of the Data Protection Act.

The Data Controller therefore has both the rights and the obligations to make decisions about the purposes and the means for processing.

The Data Controller is responsible for ensuring that there is a legal basis for the processing that the Data Processor is instructed to perform.

3. DATA PROCESSOR WORKS AFTER INSTRUCTIONS

The Data Processor may only process personal data according to documented instructions from the Data Controller, unless required under EU law or the national law of the Member States to which the Data Processor is subject. In that case, the Data Processor shall notify the Data Controller of this legal requirement before processing unless that court prohibits such notification for reasons of important social interest, cv. Article 28 (2) 3(a).

The Data Processor immediately informs the Data Controller if an instruction, in the opinion of the Data Processor, is contrary to the Data Protection Regulation or Data Protection Provisions in other EU law or national law of the Member States.

4. CONFIDENTIALITY

The Data Processor ensures that only the persons currently authorized to do so have access to the personal data processed on behalf of the Data Controller. Access to the information must therefore be immediately terminated if the authorization is deprived or expired.

Only persons authorized for access to personal data may be authorized to fulfill the Data Processor´s obligations to the Data Controller.

The Data Processor ensures that the persons authorized to process personal data on behalf of the Data Controller have committed themselves to confidentiality, or are subject to appropriate statutory confidentiality.

At the request of the Data Controller, the Data Processor should be able to demonstrate that the relevant employees are subject to the aforementioned confidentiality obligation.

5. SECURITY OF PROCESSING

The Data Processor initiates all measures required by Article 32 of the Data Protection Regulation, which inter alia it is apparent that, taking into account the current level, the implementation costs and the nature, scale, coherence and purpose of the treatment concerned, as well as the risks of varying probability and seriousness of the rights and freedoms of natural persons, appropriate technical and organizational measures must be implemented to ensure a level of safety fits these risks.

The above obligation implies that the Data Processor must carry out a risk assessment and then take measures to address identified risks. Among other things, the following measures may include, inter alia, the following:

a. Pseudonymization and encryption of personal data
b. Ability to ensure continued confidentiality, integrity, accessibility and robustness of treatment systems and services
c. Ability to restore timely availability and access to personal data in case of a physical or technical incident
d. A procedure for periodic testing, assessment and evaluation of the effectiveness of technical and organizational measures to ensure treatment safety.

In connection with the above, the Data Processor must implement at least the level of security and the measures specified in Appendix C of this agreement.

In connection with the Data Controller or Data Processor´s subsequent requirement for establishing additional security measures, it will be apparent from the parties´ “Main Agreement” or from Appendix D of this agreement.

6. USE OF SUB DATA PROCESSORS

The Data Processor must comply with the conditions set out in Article 28 (1) of the Data Protection Regulation 2 and 4, to use another Data Processor (Sub Data Processor).

The Data Processor must thus not use another Data Processor (Sub Data Processor) to fulfill the Data Processor Agreement, without prior specific or general written approval from the Data Controller.

In the case of general written approval, the Data Processor must notify the Data Controller of any planned changes regarding the addition or replacement of other Sub Data Processors, thereby giving the Data Controller the opportunity to object to such changes.

The Data Controller´s terms and conditions for the Data Processor´s use of any Sub Data Processors are contained in Appendix B of this agreement.

The Data Controller´s possible approval of specific Sub Data Processor is listed in Appendix B of this agreement.

When the Data Processor has the Data Controller´s authorization to use a Sub Data Processor, the Data Processor provides to impose on the Data Processor the same data protection obligations as those set forth in this Data Processor Agreement through a contract or other legal document under EU law or national law of the Member States in particular providing the necessary guarantees that the Sub Data Processor will implement the appropriate technical and organizational measures in such a way, that the processing meets the requirements of the Data Protection Regulation.

The Data Processor is thus responsible for – through the conclusion of a Sub Data Processor agreement – to impose any Sub Data Processor at least the obligations that the Data Processor itself is subject to under the data protection rules and this Data Processor Agreement and its appendices.

The Data Processor Agreement and any subsequent changes thereto will be sent to the Data Controller, upon request by the Data Controller, in order to ensure that a valid agreement has been entered into between the Data Processor and the Subdataprocessor. Any commercial terms, such as prices that do not affect the data protection content of the Sub Data Processor Agreement, should not be sent to the Data Controller.

The Data Processor must in its agreement with the Sub Data Processor insert the Data Controller as a beneficiary third party in the event of the bankruptcy of the Data Processor, so that the Data Controller may enter into the Data Processor´s rights and apply them to the Subdataprocessor, for example so the Data Controller can instruct the Subdataprocessor to delete or retrieve information.

If the Subdataprocessor does not comply with its data protection obligations, the Data Processor remains fully liable to the Data Controller for the fulfillment of the Sub Data Processor obligations.

7. TRANSFER OF INFORMATION TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS.

The Data Processor may only process personal data by documented instructions from the Data Controller, including as regards the transfer (transfer, transfer and internal use) of personal data to third countries or international organizations, unless required under EU law or the national law of the Member States as the Data Processor is subject to. In that case, the Data Processor shall notify the Data Controller of this legal requirement before processing unless that court prohibits such notification for reasons of important social interest, cf. Article 28 (2) 3(a).

Without the Data Controller´s instruction or approval, the Data Processor – within the framework of the Data Processor Agreement – can, among other things, not do the following:

a. Pass personal data to a Data Processor in a third country or in an international organization
b. Leave the processing of personal data to a Sub Data Processor in a third country
c. Handle the information to another of the Data Processor´s departments located in a third country.

The Data Controller´s possible instruction or approval of the transfer of personal data to a third country, will appear from Appendix C of this agreement.

8. ASSISTANCE TO THE DATA CONTROLLER

The Data Processor, taking into account the nature of the processing, shall, as far as possible, assist the Data Controller by appropriate technical and organizational measures, with the obligation of Data Controller to respond to requests for the exercise of the data subjects´ rights as laid down in Chapter 3 of the Data Protection Regulation.

This implies that, as far as possible, the Data Processor shall assist the Data Controller in connection with the Data Controller being responsible for ensuring compliance with:

a. The disclosure obligation for collecting personal data from the data subject
b. The disclosure obligation whose personal data have not been collected by the data subject.
c. The data subject´s right of insight
d. The right to rectification
e. The right to delete “the right to be forgotten”
f. The right to limitation of treatment
g. Notification obligation in connection with the correction or deletion of personal data or limitation of treatment
h. The right to data portability
i. The right of objection
j. The right to object to the result of automatic individual decisions, including profiling.

The Data Processor assists the Data Controller in ensuring compliance with the Data Controller´s obligations pursuant to Article 32-36 of the Data Protection Regulation, taking into account the nature of the processing and the information available to the Data Processor, cf. Article 28 3 (f).

This implies that, in consideration of the nature of the processing, the Data Processor must assist the Data Controller in ensuring that the Data Controller is responsible for ensuring compliance with:

k. The obligation to implement appropriate technical and organizational measures to ensure a level of safety that fits the risks associated with treatment
l. The obligation to report personal data breach to the Supervisory Authority (Data Inspectorate) without undue delay and, if possible, within 72 hours after the Data Controller has been notified of the breach, unless it is unlikely that the breach of personal data security implies a risk to natural person's rights or freedoms.
m. The obligation to – without undue delay – notify the registered data breach of personal data security when such a breach is likely to entail a high risk of the rights and freedoms of natural persons
n. The obligation to conduct an impact assessment on data protection if one type of treatment is likely to entail a high risk of natural persons´ rights and freedoms
o. The obligation to consult the supervisory authority (Data Inspectorate) before processing if an impact assessment on data protection shows, that the treatment will lead to high risk in the absence of measures taken by the Data Controller to limit the risk

Any adjustment / settlement of the parties to the agreement or the like in connection with the Data Processor´s assistance to the Data Controller will appear from the parties´ "Main Agreement" or from Appendix D of this agreement.

9. UNDERSTANDING ON PERSONALITY SAFETY

The Data Processor shall inform the Data Controller without undue delay after being aware that there has been a violation of the personal data security, at the Data Processor or any Sub Data Processor.

The Data Processor´s notification to the Data Controller should, if possible, be made within 24 hours after it has become aware of the violation so that the Data Controller is able to comply with its obligation to report the breach to the supervisory authority within 72 hours.

In accordance with paragraph 10 of this agreement, the Data Processor – in consideration of the nature of the processing and the information available to it – shall assist the Data Controller in reporting the breach of the supervisory authority. This may mean that the Data Processor shall assist in providing the following information, as provided for in Article 33 (3) of the Data Protection Regulation. 3, to the supervisory authority

a. The nature of the breach of personal data security including, if possible, the categories and the approximate number of registered persons, as well as the categories and the approximate number of personal data records concerned.
b. Probable consequences of the breach of personal data security
c. Measures taken or proposed to address the breach of personal data protection, including where appropriate, measures to limit its possible harmful effect.

10. DELETATION AND DELIVERY OF INFORMATION

Upon termination of the processing services, the Data Processor is obliged to delete or retrieve all personal data to the Data Controller, as well as to delete existing copies, unless the European Union or national law prescribes the retention of personal data.

11. MONITORING AND AUDIT

The Data Processor shall make available to the Data Controller all information necessary for detecting the compliance of the Data Processor with Article 28 of this Data Protection Regulation and this Agreement, allowing and contributing to audits, including inspections carried out by the Data Controller or other auditor authorized by the Data Controller.

The detailed procedure for the Data Controller´s supervision of the Data Processor is set out in Appendix C of this agreement.

The Data Controller´s supervision of any Sub Data Processor is based on the Data Processor. The detailed procedure for this is stated in Appendix C of this agreement.

The Data Processor is required to provide authorities with access to the Data Controller and Data Processor facilities, or representatives acting on behalf of the Authority, access to the physical facilities of the Data Processor against duly credentials.

12. AGREEMENTS OF OTHER PARTIES

Any (specific) regulation of the consequences of the parties' breach of the Data Processor Agreement will be stated in the parties´"Main Agreement" or in Appendix D of this agreement.

Any regulation of other relations between the parties will be apparent from the parties´ "Main Agreement" or from Appendix D of this agreement.

13. IMPACT AND DISPOSAL

This agreement shall enter into force upon the signature of both parties.

The agreement may be renegotiated by both parties if the law changes or inconsistencies in the agreement give rise to this.

Any adjustment / agreement of the parties regarding remuneration, conditions or the like in connection with changes to this agreement will appear from the parties´ "Main Agreement" or from Appendix D of this agreement.

Termination of the Data Processor Agreement may be in accordance with the termination conditions, including termination notice, as stated in the "Main Agreement".

The agreement is valid for the duration of the treatment. Regardless of the termination of the “Main Agreement” and / or the Data Processor Agreement, the Data Processor Agreement will remain in effect until termination of the processing and the deletion of the data by the Data Processor and any Sub Data Processor.

14. SUBSCRIPTIONS

On behalf of the Data Controller:		On behalf of the Data Processor:	
Name:		Name:	Anders Frost
Date:		Date:	30-03-2023
Job Title:		Job Title:	Chairman & Founder
Phone number:		Phone number:	+45 5151 2271
E-mail:		E-mail:	Anders.Frost@capana.dk

15. CONTACT PERSONS OF THE DATA CONTROLLER AND DATA PROCESSOR

The parties can contact each other via the following contacts:

The parties are required to keep each other informed of changes regarding the contact person.

On behalf of the Data Controller:		On behalf of the Data Processor:	
			
Name:		Name:	Anders Frost
Job Title:		Job Title:	Chairman & Founder
Phone number:		Phone number:	+45 5151 2271
E-mail:		E-mail:	Anders.Frost@capana.dk

capana

Data Processor Agreement

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Anders Frost		2023.01.01	2023-01-01	Commercial-in-confidence

capana

DATA PROCESSOR AGREEMENT

INFORMATION ON THE TREATMENT

APPENDIX A

capana

Databehandleraftale

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Bente Pedersen		Appendix A	2018-05-25	Commercial-in-confidence

1. INFORMATION ON THE TREATMENT

1.1. Purpose

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is, that the Data Processor can collect and treat the relevant personal information which is relevant for performing the assignment given by the Data Controller.

1.2. Grade

The Data Processor's processing of personal data on behalf of the Data Controller primarily concerns that the Data Processor makes the system available to the Data Controller, thereby storing personal data about the Data Controller members on the company's servers.

1.3. Types

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

- Personalia
- Demographics
- Behavioral data
- Customer account data
- Products and purchases

1.4. Duration

The Data Processor's processing of personal data on behalf of the Data Controller may commence after the entry into force of this Agreement. The processing is not limited to time and time until the agreement is terminated or terminated by one of the parties.

1.5. Access to data

The following consultants will have access to the Data Controller's data and will treat them confidentially.

capana

Databehandleraftale

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Bente Pedersen		Appendix A	2018-05-25	Commercial-in-confidence

Name of the Consultant	Phone number	Mail address

capana

DATA PROCESSOR AGREEMENT

CONDITIONS FOR THE DATA PROCESSORS USE OF SUB DATA PROCESSORS

APPENDIX B

capana

Data Processor Agreement

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Bente Pedersen		Appendix B	2018-05-25	Commercial-in-confidence

1. TERMS AND CONDITIONS OF DATA PROCESSORS USE OF SUB DATA PROCESSORS AND LIST OF APPROVED SUB DATA PROCESSORS.

1.1. Conditions

The Data Processor has the data manager's general authentication to use Sub Data Processor. However, the Data Processor must notify the Data Controller of any planned changes regarding the addition or replacement of other Sub Data Processor, thereby giving the Data Controller the opportunity to object to such changes. Such notification shall be the Data Controller at least 3 months prior to use or the amendment shall take effect. If the Data Controller opposes the changes, the Data Controller must notify the Data Processor within 14 days of receiving the notification. The Data Controller can raise objections only if the Data Controller has reasonable, concrete reasons for this.

1.2. Approved Sub Data Processors

At the entry into force of the Data Processing contractor, the Data Controller has approved the use of the following Sub Data Processor:

Name	CVR-nr.	Address	Description of treatment

capana

DATA PROCESSOR AGREEMENT

INSTRUCTIONS FOR THE TREATMENT OF PERSONALIZATIONS

APPENDIX C

capana

Data Processor Agreement

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Bente Pedersen		Appendix C	2018-05-25	Commercial-in-confidence

1. INSTRUCTIONS FOR THE TREATMENT OF PERSONALIZATIONS

1.1. Treatment instructions

The Data Processor's processing of personal data on behalf of the Data Controller is done by the Data Processor performing the specific tasks described in the main agreement between the parties.

1.2. Security of processing

The level of security must reflect the processing of a large amount of personal data covered by Article 9 of the Data Protection Regulation on "special categories of personal data", which means that a "high" level of security must be established. The Data Processor is then entitled and obliged to make decisions about the technical and organizational security measures to be used to create the required (and agreed) security level around the information.

However, the Data Processor must - in all cases and at least - implement the following measures agreed with the Data Controller (based on the risk assessment performed by the Data Controller) by describing the following possible requirements regarding:

Demand	Data Responsible Requirements (tick box)
Personal information data is stored on encrypted servers / PCs	
The ability to ensure continued confidentiality, integrity, availability and robustness of treatment systems and services.	
The ability to rectify the availability of and access to personal data in the event of a physical or technical incident.	
Procedures for regular testing, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure treatment safety.	
Access to data via the Internet	
Protection of data in which they are transmitted.	

Protection of data where they are stored.	X
Physical protection of sites where personal data are processed.	
Use of home and remote workplaces.	X
Logging.	

1.3. Storage period and delete routine

The personal data is stored with the Data Processor until the Data Controller requests the information deleted or returned.

1.4. Location of treatment

Processing of the personal data contained in the agreement may not, without the Data Controller's prior written consent, create other locations than the data processor's address in Aalborg and at the home address of the relevant named consultant in the Data Processing Agreement.

1.5. Instructions or approvals regarding the transfer of personal data to third countries

If the Data Controller has not provided an instruction or approval for the transfer of personal data to a third country in this section or subsequent written notice, the Data Processor may not make such a transfer within the framework of the Data Processing Agreement.

1.6. Further procedure for the Data Controller’s supervision of the processing performed by the Data Processor

The Data Controller or a representative of the Data Controller is allowed to supervise, including physical compliance with the Data Processor, when the Data Controller assesses a need for this.

The Data Controller's possible expenses in connection with physical supervision shall be borne by the Data Controller himself.

1.7. Further procedure for the supervision of the treatment performed with any Sub Data Processor

The Data Processor or a Data Processor Representative has access to oversight, including physical supervision, at the Sub Data Processor, when the Data Processor considers it necessary.

capana

DATA PROCESSOR AGREEMENT

PARTIES' REGULATION OF OTHER MATTERS

APPENDIX D

capana

Data Processor Agreement

Document issued by:	Project/Client reference:	Document revision:	Document issue date:	Confidentiality level
Bente Pedersen		Appendix D	2018-05-25	Commercial-in-confidence

1. PARTIES' REGULATION OF OTHER MATTERS