Data Processing Agreement
“DPA”

between

Clinic Org. no.

«Controller»

…….

and

Calpro AS Org. nr. 966 291 281

…….

«Processor»

If the parties have executed a Data Management Agreement, the Date Management Agreement will take precedence over this Agreement as regards data protection matters

1. SCOPE OF THE AGREEMENT

This DPA (hereafter "the DPA") intends to regulate the rights and responsibilities of the Controller and Processor in accordance with Applicable data protection law. The parties acknowledge that the Applicable data protection law requires a DPA between a controller and a processor regarding the processors processing of Personal data on behalf of the controller. The DPA shall ensure that the Personal data regarding the data subjects will not be misused or unlawfully Processed or disclosed.

The DPA regulates the Processor's Processing of Personal data on behalf of the Controller, including collecting, recording, alignment, storing, registering of extracts, disclosure or combinations of these.

2. DEFINITIONS AND INTERPRETATIONS

Controller is the party that determines the purposes and means of the Processing of Personal data.

Processor: The party that Processes Personal data on behalf of the Controller.

Applicable data protection law: Means the Norwegian Personal Data Act, the Norwegian Personal data regulation, the EU Data Protection Directive 95/46/EC, or other EU legislation that may be promulgated, any national or internationally binding data protection laws or regulations applicable at any time during the term of this DPA. "Applicable data protection laws" includes any binding guidance, opinions or decisions of regulatory bodies, courts or other bodies, as applicable, as well as the forthcoming European Union General Data Protection Regulation (hereinafter referred to as "GDPR") when it enters into force on the 25th May 2018.

Personal data: Means any information relating to an identified or identifiable natural person.

Special categories of personal data: Means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing: Means any operation or set of operations that is performed on Personal data. Examples are collecting, recording, alignment, storing, register extracts, or combinations of these.

Data subject: The identified or identifiable natural person that the Personal data is related to.

3. PURPOSE

The parties have entered into a license agreement for the use of CalproSmart (hereafter "License agreement"), thus the Processor will Process Personal data on behalf of the Controller. The DPA regulates the rights and responsibilities of the parties regarding the Processor's Processing of Personal data on behalf of the Controller.

The Processor shall provide and operate CalproSmart. Thus, the Processor will process Personal data about patients and doctors and other employees at health institutions that are using CalproSmart. An overview of the data flow is set out in Appendix 1 to the DPA.
The parties have entered into a License agreement which describes the services the Processor shall provide.

The purpose of the Processing is to enable the Controller to monitor the patient's medical condition.

The Processor will process the following Personal data:

The patient's

- Name
- Personal identification number
- Address
- Telephone number
- E-mail address
- Test result
- Sex
- Test frequency
- Time spent on sampling
- Phone model
- App version, browser, batch number and expiration date
- Language

The Processor shall keep an updated overview of the current Processing activities at all times.

The Processor will Process special categories of Personal data, which requires an increased focus on a safe processing of the Personal data.

The Processor shall only process Personal data as follows:

- collecting, recording, logging, alignment, store, register extracts, or combinations of these

The Processor undertakes not to process the Personal data for its own- or any other purpose than those described herein.

4. THE PROCESSORS RESPONSIBILITIES

The Processor warrants that it has implemented, and will and continue to implement under the term of this DPA, the appropriate technical and organizational measures to ensure that the processing of Personal data under the DPA will comply with the requirements of Applicable data protection law.

The Processor undertakes to only process Personal data in accordance with documented routines and instructions communicated by the Controller. The Processor shall nevertheless perform its services and fulfil the independent obligations of processors according to the Applicable data protection law.

The Processor shall at any time be able to document the processing of Personal data that is being conducted, and at any time be able to provide an updated list of the categories of data that is processed.

The Processor is obliged to notify the Controller promptly, and no later than 24 hours after the Processor has gained knowledge of a discrepancies or Personal data breach. The Controller is responsible for sending a discrepancy notice to the Data Protection Authority,

and the Processor shall assist the Controller with information about the discrepancy or data breach. The Controller is required to keep records of any data breach that has occurred in relation to the services provided by the Controller, and to comply with its obligations under GDPR art. 33.

The Processor is obliged to give the Controller access to its security documentation, and assist the Controller in complying with its obligations according to law and regulation. The Controller's safety requirements are set out in Appendix 2. The Processor shall have an independent responsibility to comply with relevant Applicable data protection law, including the imposed security requirements.

The Processor has an independent responsibility to notify the Controller if any Processing of Personal data under this DPA does not comply with Applicable data protection law.

The Controller is entitled to-, shall have access to, and be able to inspect the Personal data being processed, as well as the systems used for this purpose.

The Processor shall assist the Controller to fulfil its legal obligations according to the Applicable data protection law, including but not limited to, the Controller's obligations to respond to requests for exercising the Data Subject's rights to access, rectification and erasure, as well as the right to restrict the Processing and extract Personal data. The Processor shall not respond directly to requests from Data subjects, but await further instructions from the Controller. Processor may however reply to technical support questions directed to support@calpro.no.

The Processor shall provide the Controller with the necessary assistance regarding privacy impact assessments and the handling of data breaches.

The Processor may not, without prior instructions from the Controller, transfer or in any other way disclose Personal data or any other information relating to the processing of Personal data to any third party.

Personal data and documentation that the Processor get access to under this DPA is confidential. Confidentiality applies after the termination of the DPA as well.

5. THE CONTROLLER'S RESPONSIBILITIES

The Controller is the owner of the data and determines the purpose and means for processing them. It is the Controller's responsibility to obtain the necessary legal basis for the processing of the relevant Personal data, including the special categories of Personal data that is Processed by CalproSmart.

Any special security measures or requirements on the Processor this will be described in Appendix 2.

The Controller is responsible for complying with the Data subject's rights, hereunder the right to access, rectification and erasure, as well as the obligation to data minimization and privacy by design and by default. The Controller shall facilitate compliance with these obligations and is responsible to ensure that the services and solutions are in accordance with the Applicable data protection law.

6. SUB PROSESSORS

The Processor uses third party subcontractors (hereafter «Sub processors») that are engaged by the Processor, and will, as part of the subcontractor's role of delivering the services, Process Personal data on behalf of the Controller. The Sub processors are:

- Netcompany AS
- Isky AS

The Controller hereby accepts that the Processor may engage the Sub processors mentioned above. In order to engage any other Sub processors, a prior written consent from the Controller is required before the processing of Personal data starts.

The Processor shall enter into written agreements with its Sub processors that requires the Sub processors to comply with corresponding obligations to those contained in the DPA. The Controller is entitled to receive copies of the relevant terms of the Processor's agreement with its Sub processors which involves Personal data and security.

Anyone who performs assignments where Personal data is processed on behalf of the Controller must know the Processor's contractual and statutory obligations and fulfill the terms thereof. The Processor will be liable to the Controller if the Sub processors do not fulfill the obligations arising from this DPA.

7. INFORMATION SECURITY AND CONFIDENTIALITY

The Processor shall ensure the appropriate level of IT security, including system security, confidentiality, integrity, administration of access and ensure that no one receives unauthorised access to Personal data. The Processor must be able to document this at any time.

The Processing involves special categories of Personal data. The Personal data must therefore be encrypted and pseudonymised when possible. The Processor shall have a routine for restoring the availability and access to the Personal data for the Controller and the Data subject in the event of a physical or technical incident.

Only the Sub processors that needs access to the Personal data in order to perform their service to the Processor of behalf of the Controller shall be given access to the Personal data. Anyone with access to Personal data must commit themselves to confidentiality or be under proper statutory obligation of confidentiality. This duty shall survive the expiry or termination of the DPA.

The Processor shall establish and maintain security measures that through risk assessment has been identified as necessary.

The Processor shall not transfer any Personal data to a state that is not a member state of either the EU or the EEA, unless the Controller has given a prior written consent.

The Processor shall document routines and other measures to comply with the security requirements of the DPA. The documentation shall be made available to the Controller by request.

8. SECURITY AUDITS

The Controller and the Processor shall agree on performance of regular security audits for systems and such, regulated by this DPA.

The audit may include review of routines, random checks, more extensive on-site inspections and other appropriate measures.

9. LIMITATION OF LIABILITY

Each party's liability arising from this DPA shall be governed by the License agreement's provisions regulating the parties limitation of financial liability.

10. TERM AND DURATION

The provisions in this DPA shall apply during such time the Processor processes Personal data on behalf of the Controller.

In the event of a violation of this DPA or the Applicable data protection law, the Controller may order the Processor to cease all its processing activities with immediate effect.

11. EFFECT ON TERMINATION

The Controller owns all the Personal data Processed under this DPA, thus the Personal data cannot be transferred or used by others without the Controller's prior consent. Upon termination or expiry of this DPA, the Processor shall cease its processing activities, and, at the choice of the Controller delete or return all the Personal data to the Controller and deletes existing copies unless Applicable data protection law requires storage of the Personal data. The Processor shall ensure that any Sub processors do the same.

Upon request by the Controller, the Processor shall provide electronic copies of content in databases and the like with data included.

Upon request by the Controller, the Processor shall document in writing that deletion and destruction is executed in accordance with this DPA within a reasonable time after the DPA's termination or expiry.

12. NOTICES

All notices, requests, claims, demands and other communications under this DPA from one Party to the other shall be in writing addressed to:

On behalf of the Controller: Clinic admin at registered clinic

On behalf of the Processor: Calpro As

Arnstein Arnebergsvei 30

1366 Lysaker.

13. DISPUTE RESOLUTION

The parties hereby agree to the jurisdiction of Asker og Bærum tingrett, Norway. This also applies after the termination or expiration of this PDA.

***

[Place and date]

[Name of clinic]	Calpro AS
_____	_____
Name:	Name: Anne Thjømøe
Position:	Position: CEO