Data Processing Agreement

Between the customer of Datalogisk/Agrinavia, hereinafter mentioned as the "**Data Controller**"

and

Datalogisk A/S (Agrinavia), Company Registration No. in DK78871911 hereinafter mentioned as the "**Data Processor**"

(The Data Controller and the Data Processor are hereinafter individually referred to as a **"Party"** and jointly, the **"Parties")**

The Parties have concluded this Data Processing Agreement ("**Agreement**"):

1. Personal Data and Data Processing

1.1 As part of the Data Processor's services to the Data Controller, the Data Processor will process personal data on behalf of the Data Controller. The Data Processor processes the categories of personal data ("**Personal Data**") for the purposes and by carrying out the activities, as laid out in **Appendix A**.

1.2 The Data Processor may only store Personal Data within the EU/EEA and is not entitled to transfer any such data to countries outside the EU/EEA without the prior written acceptance of the Data Controller.

2. Instructions and confidentiality

2.1 The Data Processor may only process the Personal Data in compliance with documented instructions from the Data Controller. If, in exceptional cases, the Data Processor is instructed to process the Personal Data, including transferring the Personal Data to a third country or an international organisation, and this does not follow from instructions of the Data Controller, but is required by EU or the member state law to which the Data Processor is subject, the Data Processor must notify the Data Controller of such legal requirements before commencing the processing unless such notification is prohibited on important grounds of public interest.

2.2 The Data Processor may not process the Personal Data for its own purposes, unless explicitly agreed in this Agreement.

2.3 The Data Processor is bound by confidentiality, and the Data Processor may not without authorisation copy, disclose or use the Personal Data. The Data Processor must ensure that all employees authorised to process the Personal Data have assumed a contractual confidentiality obligation or are subject to a statutory obligation of secrecy.

2.4 The Data Processor must ensure that access to the Personal Data is limited to employees who need such access to perform their work.

3. Security, etc.

3.1 In order to protect the Personal Data, the Data Processor must implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the Danish Act on Processing of Personal Data and, as of 25 May 2018, EU Regulation 2016/679 on General Data Protection (the "**General Data Protection Regulation**"). The nature of such measures must take into account the technical level at the relevant time, the expenses, nature, scope, context and purposes of the processing and the risks to the rights of natural persons.

3.2 The Data Processor must comply with the security instructions set out in **Appendix B**.

4. Sub-processors

4.1 Subject to clause 4.3, the Data Processor is hereby authorised to use sub-processors without obtaining any further written approval from the Data Controller provided that the Data Processor notifies the Data Controller of the identity of the potential sub-processors (and their potential sub-processors) before entering into any agreement with any such sub-processors and provided that the Data Controller is given the opportunity to object to the use of the sub-processor.

4.2 Notification and the opportunity to object pursuant to clause 4.1 must also be given in case of potential, planned changes concerning the addition or replacement of sub-processors or the discontinuation of the use of sub-processors. An objection must reach the Data Processor no later than seven days after the Data Controller's receipt of the notification.

4.3 It is a pre-condition for appointing a sub-processor that the Data Processor and the sub-processor enter into an agreement under which the sub-processor accepts the same data protection obligations and contractual terms as those set out in this Agreement, including, but not limited to, the sub-processor's obligation to implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the General Data Protection Regulation and that the sub-processor only acts in accordance with documented instructions of the Data Controller.

4.4 The data processor is liable to the Data Controller for any sub-processors to the same extent as the Data Processor is liable for its own actions and omissions.

5. Assistance to the Data Controller

5.1 The Data Processor must assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 32-36 of the General Data Protection

Regulation and any other applicable data protection and information security legislation, i.e. security measures, notification of supervisory authorities, notification of Individuals, preparation of data protection impact assessments and prior consultation of the supervisory authorities.

5.2 Taking into account the nature of the processing and the information available to the Data Processor, the Data Processor must implement appropriate technical and organisational measures to assist the Data Controller in complying with the Data Controller's legal obligations under Chapter III of the General Data Protection Regulation, i.e. answering requests from Individuals exercising their legal rights, including, but not limited to, the rights of access to, rectification or deletion of Personal Data, restriction of the processing of Personal Data, data portability and the right to object to automated individual decision-making, including profiling.

5.3 The Data Processor must immediately notify the Data Controller of any personal data breaches.

5.4 The Data Processor must immediately inform the Data Controller if the Data Processor finds that an instruction violates the General Data Protection Regulation or any other data protection provisions under EU or member state law.

6. Demonstration of compliance, audits, etc.

6.1 The Data Processor must upon request make available to the Data Controller all information necessary to demonstrate compliance with the obligations stipulated in this Agreement and applicable data protection legislation.

6.2 The Data Processor must allow for and contribute to audits, including inspections, conducted by the Data Controller or auditors authorised by the Data Controller, the Danish authorities or any other competent jurisdiction. The relevant auditor must be subject to confidentiality, either under an agreement or by law.

7. Liability and indemnity

7.1 The Parties incur liability under the general principles of Danish law.

7.2 The liability of either Party shall not exceed 50.000.000 DKK.

8. Severability

8.1 Should any provision of this Agreement be held unenforceable, illegal or invalid, such provision or provisions may by good faith negotiations or interpretation be replaced by provisions that to the widest extent possible give effect to the intent and enforcement of the original provisions. If that is not possible, such provision must to that extent be deemed not to form part of this Agreement. All other provisions as well as terms and conditions of this Agreement remain in full force and effect.

9. Term and termination

9.1 This Agreement takes effect when entered into and remains in force until terminated by either of the Parties. However, the Agreement remains in force for as long as the Data Processor is processing the Personal Data, even if such processing takes place after the termination of this Agreement.

9.2 At the termination of this Agreement, the Data Processor may not cease the processing of the Personal Data until the Personal Data have either been returned to the Data Controller on a medium at the choice of the Data Controller or transferred to a new data processor at the choice of the Data Controller. Following this, the Data Processor must delete all existing copies of the Personal Data unless mandatory EU or member state law requires continued storage of the Personal Data.

9.3 If, after the termination of this Agreement, there is doubt as to whether the Data Processor has deleted all the Personal Data, the Data Controller may request the Data Processor to provide, at the Data Processor's own expense, an audit statement confirming that the data processing is no longer taking place and that the Personal Data have been deleted.

10. Signatures

10.1 This Agreement is signed in two identical original counterparts of which each Party receives one.

Place:

Date:

For [Party]:

[Name]	[Name]

Sub-Appendix A – Information about the processing operation

1. Data subjects and personal data

1.1 The Data Processor processes the following categories of data subjects ("Data Subjects") and the following categories of personal data ("Personal Data") about the Data Subjects on behalf of the Data Controller:

Category	Categori 1
Non-sensitive categories of personal data	Name, telephone number, email and postal addresses and subscription number, IP adress

2. Purpose

2.1 The Data Processor's processing of Personal Data for the Data Controller is carried out for the following purpose:

- the data controller can use Datalogisk/Agrinavia software (Agrinavia Field, Agrinavia Map and Agrinavia MOBILE), owned and managed by the data processor, to collect and process information about the data controller.

3. Data processing activities/nature of processing operation

3.1 The Data Processor's processing of Personal Data for the Data Controller is carried out through the following activities:

- By storing Personal Data and securing the availability, integrity and confidentiality of systems
- By providing remote service to the Data Controller's users of Agrinavia Software
- By preparing marketing measures in the form of electronic newsletters]

4. Duration

4.1 The Parties expect that the Data Processor will be processing the Personal Data for as long as the Agreement is automatically renewed, and the data controller remains as customer].

5. Deletion

5.1 During the Term of the Agreement, the Data Processor is to delete Personal Data five years after termination of user access to Agrinavia Software

6. Recipients

6.1 In addition to any sub-processors set out in **Sub-Appendix A**, the Data Processor may disclose Personal Data to the following recipients in connection with the processing operation:

☐ No recipients

☒ Recipients are set out in the table below

Name of recipient	Address (including country) of the recipient	Categories of Personal Data which may be disclosed to the recipient	Purpose of the disclosure to the recipient
Curanet A/S	Højvangen 4 DK-8660 Skanderborg	Personal date as described in 1.1	User management and invoicing

Sub-Appendix B – Security instructions

1. Security measures

1.1 The Data Processor must ensure that the Personal Data are deleted from every IT-system, archive etc. when continued storage no longer serves a fair purpose, see separate instructions from the Data Controller.

1.2 The Data Processor must inform relevant employees of and train them in confidentiality relating to the processing of the Personal Data and must ensure that the processing complies with the purposes of this Agreement and the instructions of the Data Controller.

1.3 Furthermore, the Data Processor must take the following measures:

1.3.1 Physical security: When not used, the equipment and the units must be locked and/or locked away.

1.3.2 Back-up copies: The Personal Data must be backed up routinely. The copies must be stored separately and with due care to ensure that the Personal Data can be restored.

1.3.3 Control of access: Access to the Personal Data must be limited by technical control of access. User-ID and password must be personal and may not be transferred. Procedures for the granting and termination of access must be available.

1.3.4 Communication of data: Communication of the Personal Data must take place on secure lines. Personal Data transferred outside a closed network controlled by the Data Controller must be protected by encryption.

1.3.5 Destruction of hardware: When equipment or mobile units containing Personal Data are no longer used to process Personal Data, the Personal Data must be permanently deleted from the equipment to ensure that the data cannot be restored