DKE CONNECTIVITY PLATFORM DATA PROCESSING AGREEMENT

This DKE Connectivity Platform Data Processing Agreement (the "**DPA**") stipulates the details of the processing of personal data in connection with the Connectivity Platform.

The member taking note of and accepting this DPA (the "**Customer**") is, subject to the terms of the Main Agreement, entitled to use the services of DKE, in particular, with regard to the use of the Connectivity Platform. To the extent the services to be provided by DKE under the Main Agreement include and/or require the processing of Personal Data, the processing of such data shall be carried out exclusively on the basis of this DPA and on behalf of the Customer.

1. DEFINITIONS

"**Agreement**" means this DPA and the Main Agreement.

"**App(s)**" means the software applications developed or to be developed by the Customer, which can be used by End Users after their connection to the Connectivity Platform. "App(s)" within the meaning of the DPA shall also be deemed to include the use of communication units (CUs), including any terminal or telemetry connections, which themselves establish and/or maintain data traffic to the Connectivity Platform.

"**App Instances**" means the software clients of an App executed and used by End Users.

"**Association**" means the "DKE-Data agrirouter" association (after registration the "DKE-Data agrirouter e.V.") based in Osnabrück, Germany.

"Connectivity Platform" means the cloud-based IT solution currently marketed under the name "agrirouter" for the connection of and the data exchange between agricultural machines, equipment, sensors, and software applications.

"**Customer**" is defined in the preamble.

"**DKE**" means the DKE-Data GmbH & Co. KG, being a German limited partnership under the Commercial Code.

"**DPA**" is defined in the preamble.

"**DSMS**" is defined in clause 4 of Sub-annex 1.

"**End User**" means farmers, agricultural contractors and holdings as well as other companies of the agricultural sector which concluded a separate agreement both with the Customer regarding the use of Apps and with DKE regarding the use of

the Connectivity Platform on the basis of the terms of use available on my-agrirouter.com or its successor website which DKE may change from time to time.

"**Main Agreement**" means the statute (*Satzung*) of the Association, as amended or restated from time to time.

"**Personal Data**" means all information relating to an identified or identifiable natural person (hereinafter referred to as "**Data Subject**").

"**SAP**" is defined in clause 7.1 of this DPA.

2. SPECIFICATION OF THE COMMISSION

2.1. The subject matter of the commission is set out in the Main Agreement. The duration of the commission (term) corresponds to the Customer's membership ("*Mitgliedschaft*") in the Association, as set out in the Main Agreement. The nature and purpose of the processing of Personal Data by DKE for the Customer are set out in the Main Agreement.

2.2. Under the Agreement, DKE acts as a processor of the Customer or, if the Customer itself is a processor of End Users, as a sub-processor of the Customer.

2.3. The contractually agreed data processing will take place both within member states of the European Union or other contracting states to the Agreement on the European Economic Area and in third countries. The specific requirements of Art. 44 et seqq. GDPR are fulfilled with respect to each transfer to a third country. An adequate level of protection in third countries is provided by way of standard contractual clauses (Art. 46 para. 2 lit. c and d GDPR) and on the basis of adequacy decisions (Art. 45 Para. 1 of the GDPR). Further provisions are set out in clause 7 of this DPA.

2.4. Personal Data undergoing processing will be all information sent or received by Apps, App Instances or machines of the Customer and/or of the End Users which relates to End Users, their employees or contractual partners and is regularly allocatable in particular to the following data types and/or data categories:

- Position, technical and agronomical data of agricultural machines and other devices, including image and video data (if any);
- Information on work carried out or planned on agriculturally cultivated land, including time schedules and workflows;
- Information on the geo-referenced application of agricultural inputs; as well as
- History data regarding information and other usage data accessed via an App.

2.5. Categories of data subjects affected by the data processing include:

- End Users;
- Employees of End Users; as well as
- Contractual partners and other third parties about which an End User enters information into an App Instance or accesses information via an App Instance.

3. TECHNICAL AND ORGANISATIONAL MEASURES

3.1. DKE must ensure the security of processing pursuant to Art. 28 para. 3 lit. c, 32 GDPR particularly in conjunction with Art. 5 para. 1, para. 2 GDPR. In summary, the measures to be taken are data security measures and measures to ensure a level of protection which is adequate to the risk in terms of the confidentiality, integrity, availability and resilience of the systems. In this context, it is necessary to consider the state of the art, the implementation costs and the type, scope and purposes of the processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR. The measures to be taken in this respect are stipulated concretely in **Sub-annex 1** to this DPA at the time of the conclusion of the Agreement.

3.2. The technical and organisational measures are subject to technical progress and development. DKE is therefore allowed to implement adequate alternative measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented and must be submitted to the Customer at any time upon request.

4. CORRECTION, RESTRICTION AND DELETION OF DATA

4.1. DKE will support the Customer with technical and organisational measures to safeguard the rights of data subjects pursuant to Art. 12 to 23 GDPR.

4.2. DKE must not on its own authority correct, delete or restrict the processing of Personal Data which is processed on commission, but only on documented instruction from the Customer (to the extent technically possible). This does not apply to the automatic deletion of Personal Data stored (cached) for a period of at least four (4) weeks.

4.3. Should a Data Subject contact DKE directly with respect to any requests for access or the correction, deletion of restriction of processing of his/her Personal Data, DKE shall forward such request to the Customer without undue delay (*unverzüglich*).

5. QUALITY ASSURANCE AND OTHER OBLIGATIONS OF DKE

In addition to complying with the provisions of this DPA, DKE must also comply with the statutory requirements referred to in Art. 28 to 33 GDPR; in this respect, it shall specifically ensures compliance with the following requirements:

5.1. Written appointment of a data protection officer performing his/her function pursuant to Art. 38 and 39 GDPR. Regularly updated contact details for the data protection officer must be made available for easy access on DKE's website.

5.2. Protection of confidentiality pursuant to Art. 28 para. 3 sent. 2 lit. b, 29, 32 para. 4 GDPR. DKE will only use employees to perform the work who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. DKE and all persons acting under its authority who have access to Personal Data shall not process that data unless on instructions from the Customer, which includes the powers granted in this DPA, unless required to do so by law.

5.3. Implementation of and compliance with all technical and organisational measures necessary for this commission pursuant to the provisions of **Sub-annex 1** "Technical and Organisational Measures".

5.4. Upon request, the Customer and DKE will cooperate with the supervisory authority in performance of its tasks.

5.5. Notification of the Customer without undue delay of any inspections and measures conducted by the supervisory authority, to the extent such measures relate to this commission. This also applies insofar as DKE is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of Personal Data in connection with the commissioned processing.

5.6. Insofar as the Customer itself is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a data subject or by a third party or any other claim in connection with the commissioned processing by DKE, DKE shall use all reasonable efforts to support the Customer.

5.7. Demonstrability of the implemented technical and organisational measures towards the Customer within the Customer's supervisory powers pursuant to clause 7 of this DPA.

6. SUBCONTRACTING

6.1. Subcontracting within the meaning of this provision are such services which relate directly to the provision of the principal service. This shall not include any ancillary services used by DKE such as telecommunication services, postal and transport services, maintenance and user services or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, in order to ensure data protection and data security of the Customer's data, DKE is obliged to conclude appropriate agreements in conformity with the law and to take control measures also with respect to outsourced services if and to the extent necessary.

6.2. The Customer consents to the commissioning of subcontractors, provided that a contractual agreement pursuant to Art. 28 para. 2 to 4 GDPR is concluded. DKE will carefully select the companies it intends to use as subcontractors, with a particular focus on the adequacy of the technical and organisational measures implemented by such companies. Furthermore, DKE must ensure that the subcontractors used by DKE comply with the provisions of this DPA and with the applicable statutory requirements and DKE must oblige the respective subcontractor to be bound by the data protection obligations laid down in this agreement between the Customer and DKE.

In case of the involvement of a new or replacement of a subcontractor, DKE will inform the Customer in advance. The Customer may object to such changes for compelling reasons. If the Customer raises an objection and DKE uses the intended subcontractor even though the subcontractor does indeed fail to comply with the requirements of the GDPR and/or of this DPA, the Customer is entitled to terminate the Agreement (limited to the part of the service provision for which the new subcontractor is used) for good cause (*aus wichtigem Grund*). This termination shall take effect on the date specified by the Customer, but no later than thirty (30) days after DKE has informed the Customer of the new subcontractor. If the Customer does not terminate within this period of thirty (30) days, the new subcontractor shall be deemed as accepted by Customer. DKE shall specifically notify the Customer regarding this legal consequence when informing the Customer about the new subcontractor.

6.3. If the subcontractor provides the agreed services outside the European Union and the European Economic Area, DKE shall ensure compliance with data protection laws by taking the measures specified in clause 2.3. The same applies where DKE intends to use service providers within the meaning of para. 1 sent. 2. Further provisions are set out in clause 7 of this DPA.

6.4. DKE provides a list of each subcontractor used for the provision of the Connectivity Platform on its website, accessible via https://go.my-agrirouter.com/dpa-subprocessors or a successor website.

6.5. DKE may replace subcontractors without notice in cases which are reasonably beyond DKE's control and which require immediate replacement for safety or other valid reasons. In this case, DKE shall inform the Customer about the replaced subcontractor without undue delay. The subcontractor shall have the same right. Clause 6.2 shall apply accordingly.

7. INTERNATIONAL DATA PROCESSING

7.1. With respect to the partial outsourcing of data processing to third countries carried out by affiliates of DKE's current subcontractor SAP Deutschland SE & Co. KG or its affiliates ("**SAP**") as a data exporter, SAP has agreed to Module 3 (Processor to Processor) of the new standard contractual clauses (EU Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on standard contractual

clauses) with each sub-processor as data importer in order to comply with data protection law.

7.2. None of the provisions of the Agreement shall, in case of conflict, be interpreted as taking precedence over any provision of the standard contractual clauses. Insofar as this DPA specifies more far-reaching provisions for audit or sub-processors, these specifications shall also apply with regard to the standard contractual clauses.

8. DOCUMENTARY EVIDENCE AND AUDITS

8.1. DKE shall ensure that the Customer is able to verify DKE's and DKE's subcontractor's (according to clause 6) compliance with its obligations pursuant to Art. 28 GDPR. DKE undertakes to provide the Customer with the required information and, in particular, to demonstrate of the implementation of the technical and organisational measures upon request.

8.2. Evidence of such measures which do not only concern the specific DPA may be provided through (i) compliance with approved rules of conduct pursuant to Art. 40 GDPR; (ii) certification pursuant to an approved certification procedure pursuant to Art. 42 GDPR; (iii) current certificates, reports or report extracts from independent entities (e.g. chartered accountants, revision departments, data protection officers, IT security departments, data protection auditors, quality auditors); or (iv) a suitable certification through an IT security or data protection audit (e.g. IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (https://de.wikipedia.org/wiki/Bundesamt_f%C3%BCr_Sicherheit_in_der_Informationstechnik) (*BSI-Grundschutz*)). This shall apply equally to evidence of measures taken by subcontractors according to clause 6.

8.3. Furthermore, the Customer has the right, after consultation with DKE, to carry out inspections or to have them carried out by auditor to be designated in each individual case who is subject to a sufficient duty to maintain confidentiality and is not in competition with DKE and/or SAP.

8.4. However, the Customer shall only be entitled to the rights pursuant to clause 8.3 if and to the extent (i) the evidence provided by DKE upon the Customer's request pursuant to clause 8.2 is insufficient; (ii) a Personal Data breach has occurred; (iii) a data protection authority requests an inspection, or (iv) mandatory data protection law grants the client a direct audit right.

8.5. Subject to deviating mandatory data protection laws, the following restrictions shall apply to inspections pursuant to clauses 8.3 and 8.4:

- A maximum of one (1) inspection is admissible within a period of twelve (12) months;
- An inspection shall last for a maximum period of three (3) working days;

- DKE must receive notice of any inspection at least ninety (90) days in advance, unless a data protection authority requests an earlier inspection; as well as

- The inspection must take place under reasonable conditions in terms of timing, location and process.

8.6. Upon completion of an inspection, the Customer will provide DKE with a copy of the inspection report.

8.7. DKE shall reasonably support the Customer's inspections. DKE also ensures such support by the subcontractors according to clause 6 insofar as necessary. DKE may claim reasonable compensation from the Customer for such support.

9. SUPPORT OF CUSTOMER; REPORTING OF BREACHES

DKE shall support the Customer in complying with the obligations contained in Art. 32 to 36 GDPR regarding the security of Personal Data, duties to report data breaches, data protection impact assessments and prior consultations. Among other things, this includes

- Ensuring an adequate level of protection through technical and organisational measures which take into account the circumstances and purposes of the processing as well as the projected likelihood and severity of a potential rights infringement due to security vulnerabilities and enable an immediate detection of any relevant infringement events;

- The obligation to report any breaches of Personal Data without undue delay, at least within 24 hours, to the Customer;

- The obligation to assist the Customer with regard to its duty to inform the Data Subject and to provide the Customer without undue delay with all relevant information in this context;

- Reasonably supporting the Customer with its data protection impact assessment; and

- Reasonably supporting the Customer with regard to prior consultations of the supervisory authority.

10. AUTHORITY OF THE CUSTOMER TO ISSUE INSTRUCTIONS

10.1. DKE shall process personal data of the Customer only in accordance with the instructions documented by the Customer. The Agreement including this DPA constitutes these documented initial instructions and any use of the cloud service constitutes further instructions. DKE shall take all reasonable measures to comply with the Customer's instructions, provided that they are required by data protection law and are technically feasible and do not require any changes to the Connectivity Platform. If the instructions are not required by data protection law

or are not technically feasible, or if DKE is unable to comply with the instructions for any other reason, or if it believes that one of the instructions violates data protection law, DKE will inform the Customer immediately (including by e-mail).

10.2. The Customer shall confirm any non-written instructions in text form without undue delay.

10.3. DKE is entitled to suspend the implementation of the respective instruction (which are generally to be addressed to DKE support (support@agrirouter.com)) until such instruction has been confirmed or amended by the Customer.

11. DELETION AND RETURN OF PERSONAL DATA

11.1. No copies or duplicates of Personal Data shall be produced without the Customer's knowledge, excluding back-up copies that are necessary to ensure proper data processing as well as any Personal Data required to comply with statutory retention requirements.

11.2. Upon termination of the Agreement or at the request of the Customer, DKE shall hand over to the Customer within ninety (90) days or, subject to prior approval by the Customer, destroy in a data-protection compliant manner all documents, processing and utilisation results as well as data sets that have come into its possession and that are connected with the contractual relationship. The same applies to any test and scrap material. The record of their deletion shall be presented upon request.

11.3. Documentation which is used to demonstrate orderly data processing in accordance with the DPA shall be stored beyond the contract duration by DKE in accordance with the respective retention periods. DKE may hand such documentation over to the Customer at the end of the contract duration to relieve DKE of this contractual obligation.

SUB-ANNEX 1 – TECHNICAL AND ORGANISATIONAL MEASURES

DKE maintains contractual relationships with several subcontractors (further defined in clause 6.1) to assist DKE with the provision and ongoing operation of the Connectivity Platform. To the extent that data processing is performed directly on and/or via the Connectivity Platform, the Technical and Organizational Measures of certain subcontractors shall apply to the data processing under the DPA, which are accordingly:

- SAP Cloud Services are used to provide the agrirouter Software Solution to the Customer and End Users. The SAP Cloud Services Technical and Organizational Measures are accessible via https://www.sap.com/about/trust-center/agreements/on-premise/data-processing-agreements.html?sort=latest_desc&tag=agreements:data-processing-agreements/agreement-technical-organizational-measures&tag=language:english or a successor website; and

- The services of subcontractors according to clause 6.4, especially used for IT service management and incident management, to ensure a consistent and reliable operation of the Connectivity Platform for the Customer and End Users. The individual service(s) provided by each subcontractor and its respective Technical and Organizational Measures are accessible via https://go.my-agrirouter.com/dpa-subprocessors or a successor website.

In this respect, DKE undertakes to comply with the respective provisions.

With respect to any additional data processing in course of the monitoring, technical support and other operational support of the Connectivity Platform as well as the processing of payments under the Main Agreement, the following technical and organisational measures shall apply:

1. CONFIDENTIALITY (Art. 32 para. 1 lit. b GDPR)

- *Physical Access Control*

  Access to the building is controlled exclusively by a mechanical locking system. The main entrance for visitors is only open when an employee is present. The key is only distributed to employees of DKE.

- *Electronic Access Control*

  Access to servers on which data is processed must only be possible after identification and successful authentication with the authorised individual's user name and password through state-of-the-art security measures. Without this authorisation, access must be denied. Generally, all access routes to Personal Data are access-protected.

In detail, the following access to the data is possible:

- *Access to the application systems via web interface*

  All users must authenticate themselves to access Personal Data – normally with their user name and password.

- *Access to the servers for administrative tasks*

  All servers require a user authentication. This is implemented by way of a user name and password.

- *Access to the data bases for administrative tasks*

  All data bases require a user authentication for access.

- *Internal Access Control*

  An authorisation concept is in place to ensure that access to the data in the system is only granted to the extent necessary for the performance of the respective task based on the internal allocation of tasks and the segregation of duties of the user. A complex authorisation concept is managed by administrators and implemented.

- *Isolation Control*

  Regulations and measures to ensure the isolated processing (storage, modification, deletion, transfer etc.) and/or storage of data and/or data carriers for different contractual purposes must be documented and applied.

- *Data Forwarding*

  To prevent any misuse of data, DKE performs adequate transmission control, which includes the following measures:

  - Encryption of data during transmission;
  - Password protection of individual documents with separate password transmission;
  - Firewall and virus protection.

2. INTEGRITY (Art. 32 para. 1 lit. b GDPR)

- *Data Transfer Control*

  Normally, data from the systems is not transferred (with the exception of subprocessing pursuant to this DPA). Should a disclosure be required as an

exception, disclosure will only be effected upon the Customer's request. The request requires DKE's approval and will be manually logged in this context.

- *Data Entry Control*

  Access to Personal Data by DKE employees is already defined in clause 5.2. Normally, there will be no access to the data beyond this defined access.

  The user groups authorised for such access are determined by DKE in advance. Any changes in this respect will be documented.

3. AVAILABILITY AND RESILIENCE (Art. 32 para. 1 lit. b GDPR)

- *Availability Control and Resilience*

  DKE's server systems are operated by subcontractors who, by the use of adequate technical and organisational measures and external certifications (e.g. ISO 27001, BSI Grundschutz), ensure that they have implemented viable resilience concepts.

- *Ability to quickly restore data availability (Art. 32 para. 1 lit. c GDPR)*

  Logging of accesses to data (especially when entering, changing, deleting data) are stored in order to detect unauthorized accesses and to quickly restore access to data in case of an incident.

4. PROCESS FOR REGULAR TESTING, ASSESSMENT AND EVALUATION (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- *Data Protection Management*

  A data protection management system ("**DSMS**") is maintained in which all data protection measures, procedures and activities are mapped. The DSMS contains data protection requirements and a comprehensive structure for mapping data protection measures. The DSMS is maintained and updated on an ongoing basis*;*

- *Incident Response Management*

  An operational and technical process for dealing with security incidents has been defined and implemented. This process ensures a uniform response and structured handling of suspected and identified security incidents. Process-related interfaces to our service providers have been established to ensure consistent handling of (potential) security incidents*;*

- *Privacy by default (Art. 25 para. 2 GDPR);* the aforementioned procedures in accordance with the applicable technical and organizational measures for the provision of SAP Cloud Services;

- *Commissioned processing control*

  For commissioned processing of Personal Data, it is necessary to ensure that the data is processed in accordance with the instructions of the Customer. For this purpose, respective powers to issue instructions have been defined at DKE.

  On-site inspections and spot checks provide additional security.

5. PROCESS FOR HANDLING OF PERSONAL DATA BREACHES

- In the event of data breaches, DKE will inform the Customer in accordance with clause 9 of the DPA.

- DKE will ensure by contract that subcontractors also comply with these obligations and will pass on corresponding notifications from them to the Customer.

6. DATA RESIDENCY

- DKE itself does not centrally store Personal Data. DKE, through the use of its subcontractors and on a best effort basis, stores Personal Data on servers located in the European Union.

7. ENCRYPTION (Art. 32 para. 1 lit. a GDPR)

- Personal Data held on work devices is stored exclusively in encrypted form. Servers for storing and processing data are operated exclusively by subcontractors who confirm in their technical and organisational measures and through external certifications (e.g. ISO 27001, BSI Grundschutz) that they have implemented state-of-the-art encryption.