Cargill EUDR Data Privacy Terms and Conditions

A. Where possible, any information will be anonymized prior to sharing between the parties or with any other party. If information disclosed is Personal Information and the Supplier is a Data Processor, the terms of the Cargill Data Processing Addendum below shall apply (Personal Information and Data Processor are defined therein).

B By providing information to Cargill, the Supplier and third parties in the supply chain agree to processing of Personal Information contained therein, including (but not limited to) geolocation/polygon plot data, for purposes including EUDR compliance. Cargill can disclose information shared as required, including (but not limited to) on request by a regulator, to customers or for audit purposes. The Supplier confirms that Personal Information has been processed in accordance with applicable law, including procuring consent from any relevant data subject, establishing any other lawful basis for the processing of Personal Information, and/or providing notice to any relevant third party about processing of Personal Information. Cargill's Business Information Notice, available at www.cargill.com/page/business-notice, provides more details on how Cargill processes personal information in a business context.

Data Processing Addendum for Data Processors

1. **Scope of Applicability.** If Supplier will Process any Personal Information, the terms of this Data Processing Addendum ("**DPA**") shall govern Supplier's Processing of such Personal Information in addition to the obligations set forth in the Terms and Conditions agreed between the parties (also referred to herein as the Agreement). In the event of any conflict or inconsistency between the terms of the Agreement and this DPA, the terms of the DPA shall prevail.

2. **Definitions. "Data Protection Laws"** means all applicable laws, rules, regulations, and ordinances relating to the Processing of Personal Information, as they now exist or are hereafter amended, including without limitation: Australia's Privacy Act 1988 (Cth) and Australian Privacy Principles or any equivalent privacy principles that take their place; Brazil's General Data Protection Law, Brazilian Law 13.709/2018 ("**LGPD**"); Canada's Personal Information Protection and Electronic Documents Act and applicable federal, provincial, and territorial privacy laws ("**PIPEDA**"); China's Cyber Security Law, Information Security Technology – Personal Information Security Specification (GB/T 35273), and Personal Information Protection Law ("**Chinese Data Protection Laws**"); the European Union's ("**EU**") Regulation 2016/679 (General Data Protection Regulation) ("**GDPR**") and relevant implementing acts by the Member States of the European Union; Japan's Act on the Protection of Personal Information (Act No. 57 of 2003, as amended); Singapore's Personal Data Protection Act 2012 and implementing measures; Switzerland's Federal Act on Data Protection of June 19, 1992, the Ordinance to the Federal Act on Data Protection ("**FADP**"), and the Ordinance on Data Protection Certification, and all Swiss laws relating to the processing of personal information under this DPA (collectively, "**Swiss Data Protection Laws**"); the United Kingdom ("**UK**") General Data Protection Regulations, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), UK Data Protection Act of 2018, and all UK laws relating to the processing of personal information under this DPA (collectively, "**UK Data Protection Laws**"); and U.S. state and federal laws and their accompanying regulations, including the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**"). **"Data Subject Request"** means any request by or on behalf of a unique person who can be identified, directly or indirectly, by Personal Information or to whom the Personal Information relates ("**Data Subject"**) to exercise the rights afforded to them by Cargill or by Data Protection Laws, including without limitation rights of access, deletion, to opt out of certain Processing, and other rights. **"Personal Information"** means information provided by or on behalf of Cargill, or collected by Supplier on behalf of Cargill, in connection with Supplier's performance of the Services pursuant to the Agreement and which relates to an identified or identifiable household or individual; for the avoidance of doubt, Personal Information shall be understood to include "personal data", "personal information", "personally identifiable information" and equivalent terms under applicable Data Protection Laws. **"Process"** and variations thereof (e.g., "Processing") means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. "**Personnel**" means the employees, agents, contractors, and representatives of a party and its subcontractors, whether or not subcontractors are affiliates of such party. "**Data Controller**," "**Data Exporter**," "**Data Importer**," "**Data Processor,**" and "**Personal Data Breach**" have the respective meanings given in the GDPR and applicable Data Protection Laws.

3. **General Privacy Obligations and Permitted Use.** With respect to the Processing of Personal Information in connection with the Agreement, Supplier will at all times comply with applicable Data Protection Laws. With respect to Personal Information, Cargill is the Data Controller and Supplier is the Data Processor. Supplier will Process Personal Information only as directed in the Agreement, this DPA, or other written instructions from Cargill (collectively, the "**Instructions**"). Supplier will not (and will ensure Supplier Personnel do not) Process Personal Information for any purpose or to any extent other than as necessary to fulfill Supplier's obligations under this Agreement or applicable Data Protection Laws, or as otherwise specified in the Instructions. If Supplier is legally required to Process Personal Information other than as specified in the Instructions, it will notify Cargill before such Processing occurs, unless the law requiring such Processing prohibits such advance notice; in that case, Supplier will notify Cargill as soon as legally permitted. Supplier will promptly notify Cargill if Supplier reasonably believes that any instruction from Cargill is inconsistent with Supplier's obligations under Data Protection Laws. Supplier will not perform its obligations under the Agreement so as to cause Cargill to breach its obligations under Data Protection Laws.

4. **Confidentiality.** Supplier will ensure that its Personnel who have access to Personal Information are both (1) informed of the confidential nature of Personal Information and obliged to keep such Personal Information confidential; and (2) aware of Supplier's duties and their personal duties and obligations under the Agreement and this DPA, including as relates to applicable Data Protection Laws.

5. **Description of Data Processing.** The subject matter of the Processing is the provision of the Services, and the Processing will be carried out for the duration of the Agreement or as otherwise specified in the Instructions. Appendices B and C to this DPA, which detail the parties, the nature and purpose of the Processing, the types of Personal Information and categories of Data Subjects, and technical and organizational security measures, form an integral part of this DPA.

6. **Return or Destruction of Personal Information.** Upon termination of the Agreement or as otherwise specified in the Instructions, Supplier will, at Cargill's election, destroy or return to Cargill all Personal Information (including all copies of Personal Information) in its possession or control (including any Personal Information subcontracted to a third party for Processing) unless otherwise required by relevant Data Protection Laws.

7. **Data Security and Breach Notification.** Supplier will implement appropriate technical and organizational security measures to ensure a

level of security appropriate to the risks presented by the Processing and nature of the Personal Information, as set forth in Appendix C, and will implement controls and policies designed to detect and promptly respond to incidents. If Supplier has knowledge of any actual or highly suspected Personal Data Breach, Supplier will: (1) promptly (but in any event within twenty-four (24) hours) report such actual or highly suspected Personal Data Breach to Cargill, including a description of the nature and anticipated consequences of the actual or highly suspected Personal Data Breach; (2) mitigate, to the extent practicable, any harmful effects of such Personal Data Breach; and (3) cooperate with Cargill in providing any notices that Cargill deems appropriate and coordinate any public statements. If any data incident involving Personal Information is attributable to a breach by Supplier or its Personnel of Supplier's obligations under this Agreement, Supplier will bear (A) the costs incurred by Supplier in complying with its legal obligations under this Agreement, and (B) in addition to any other damages for which Supplier may be liable for under this Agreement, the following costs incurred by Cargill in responding to such breach, to the extent applicable: (1) the cost of providing notice to affected individuals, (2) the cost of providing notice to government agencies, credit bureaus, and/or other required entities, (3) the cost of providing affected individuals with credit monitoring services for a specific period not to exceed twelve (12) months, to the extent the incident could lead to a compromise of the data subject's credit or credit standing, (4) call center support for such affected individuals for a specific period not to exceed thirty (30) days, and (5) the cost of any measures required under applicable law.

8. **Deidentified Data.** "**Deidentified Data**" means data that (i) cannot reasonably be used to infer information about, or otherwise be linked to, a Data Subject and (ii) is processed only in accordance with the provisions of this Clause 8 of the DPA. To the extent Cargill discloses or otherwise makes available Deidentified Data to Supplier, or to the extent Supplier creates Deidentified Data from Personal Information, Supplier shall (1) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (2) publicly commit to maintain and use such Deidentified Data in a deidentified form and to not attempt to re-identify the Deidentified Data, except that Supplier may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes are compliant with Data Protection Laws; and (3) before sharing Deidentified Data with any other party, including sub-processors, contractors, or any other persons ("**Recipients**"), contractually obligate any such Recipients to comply with all requirements of this Clause 8 of the DPA (including imposing this requirement on any further Recipients). Supplier shall remain fully liable for any failure by Supplier or its Personnel to comply with obligations relating to Deidentified Data.

9. **Cooperation, Assistance, and Audits.** Supplier shall provide reasonable cooperation and all necessary assistance to Cargill to fulfill Cargill's obligation to promptly respond to Data Subject Requests under Data Protection Laws, including but not limited to assisting Cargill in effectuating a Data Subject's right to opt out of "sales" or "sharing" of Personal Information under the CCPA or similar Data Protection Laws. Supplier shall (1) promptly (within five days) notify Cargill if Supplier, its Affiliates, or any sub-processor receives a Data Subject Request or a notification or complaint from a government authority with respect to Personal Information or the Processing activities under the Agreement; (2) not honor or effectuate a Data Subject Request without Cargill's prior written consent (which shall not unreasonably be withheld); and (3) not directly respond to any Data Subject Request or notification or complaint from a government authority, except upon the written instructions of Cargill, or as required by Data Protection Laws. Supplier shall, at no additional cost: (i) assist Cargill in ensuring compliance with Data Protection Laws, including obligations to investigate, remediate, and provide information to government authorities or Data Subjects and Personal Data Breaches without undue delay, carry out privacy impact assessments, and consult with government authorities regarding Processing that is the subject of a privacy impact assessment; (ii) make available all information necessary to demonstrate compliance with Data Protection Laws and the security obligations set out in Appendix C and (iii) allow for and contribute to audits, including physical inspections of Supplier's premises, conducted by Cargill or its representatives.

10. **Sub-processors.** Supplier will not subcontract any of its Processing operations under the Agreement to a sub-processor unless (1) it has obtained the prior written consent of Cargill to do so and (2) the sub-processor is subject to a written agreement that imposes the same obligations and restrictions on that sub-processor as are imposed on Supplier under this DPA and any obligations and restrictions contained in the Agreement relating to the Processing of Personal Information. Supplier will remain fully liable to Cargill for any sub-processor's Processing of Personal Information under the Agreement. Cargill provides a general authorization to Supplier pursuant to applicable Data Protection Laws (including Article 28(2) of the GDPR), to engage sub-processors, subject to the written agreement described above in this Clause 10. Upon written request by Cargill, Supplier will provide an up-to-date list of (i) all sub-processors involved in Processing of Personal Information; (ii) the purposes for which each sub-processor Processes Personal Information; and (iii) the jurisdictions in which each sub-processor will Process Personal Information. Cargill may, in its absolute discretion, object to the use of any sub-processor if it is not satisfied that Supplier will comply with this DPA and applicable Data Protection Laws. To the extent that any sub-processor engaged by Supplier is located in a Third Country (as defined below), Supplier will ensure that the sub-processor is bound by obligations that adequately protect Personal Information and comply with Data Protection Laws, such as by entering into Module Three of the Standard Contractual Clauses for Processor-to-Processor transfers approved by EC Decision of 4 June 2021, or appropriate processor Binding Corporate Rules.

11. **Transfers of EU, Switzerland, or UK Personal Information.** To the extent the provision of the Services involves the transfer of Personal Information located within or originating from the EU, Switzerland, or the UK—or where the Processing of such Personal Information is otherwise subject to the GDPR, Swiss Data Protection Laws, or UK Data Protection Laws—to any country outside of the EU, Switzerland, or the UK (either directly or via onward transfer) that has not been recognized by the relevant supervisory authority or under applicable Data Protection Laws as offering an adequate level of protection for personal information transferred to it from the respective jurisdiction (a "**Third Country**"), unless another valid mechanism for the lawful transfer of Personal Information recognized under applicable Data Protection Laws applies, such transfers shall be governed by the Transfer Clauses (as defined below), as specified in Appendix A. If necessary, in Cargill's opinion, the Parties agree to work in good faith to enter into any additional data privacy clauses or negotiate in good faith a solution to enable a transfer of Personal Information to be conducted in compliance with Data Protection Laws. If another valid mechanism for the lawful transfer of Personal Information recognized under applicable Data Protection Laws applies, such as Processor Binding Corporate Rules or another lawful adequacy mechanism, the transfer shall of Personal Information under this DPA shall be governed by that mechanism.

12. **Personal Information from Other Jurisdictions**. To the extent the provision of the Services involves the transfer of Personal Information from jurisdictions other than the EU, Switzerland, and the UK but which has enacted Data Protection Law(s) restricting transfers of or access to Personal Information, Supplier shall (i) cooperate with Cargill to execute any agreements and to implement all processes and measures that Cargill deems appropriate to comply with such country's Data Protection

Law(s); and (ii) Process the Personal Information in accordance with the "Additional Transfer Clauses" set forth in Appendix A, to the extent that they apply to the transfer.

13. **Protected Health Information.** If Supplier or Supplier Personnel will have access to "protected health information" (as such term is defined by the Health Insurance Portability and Accountability Act of 1996, and its implementing regulation, the Standards for Privacy of Individually Health Information, 67 Fed. Reg. Section 53, 182 et seq. (Aug. 14, 2002) and all prior and subsequent provisions and federal regulations), Supplier will execute a Business Associate Agreement in a form acceptable to Cargill. Supplier will comply with the terms of such Business Associate Agreement in performing the applicable Services.

14. **Transfers of Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, Nicaragua, Mexico, Paraguay, Peru and/or Uruguay ("Latam Countries" or individually "Latam Country") Personal Information.**

Unless otherwise agreed, Supplier will process and store all Personal Information of a Data Subject residing in a Latam Country within the respective Latam Country in which the Data Subjects reside and will not transfer, process, maintain or remotely access Cargill's Personal Information in any other jurisdiction or location without Cargill's prior consent.

Supplier will not transfer Personal Information from the Latam Countries to countries that do not provide adequate protection without first ensuring that:

(1) If the Data Importer is an Affiliate of Supplier, (A) the Data Importer, Supplier and Supplier's other Affiliates have adopted Binding Corporate Rules for data processors which govern the processing of Personal Information of the same type and for the same purposes as the Personal Information to be processed in connection with this Agreement; and (B) the Binding Corporate Rules have been approved for use by a Data Protection Authority in a Latam Country in accordance with the applicable Data Protection Laws or, in the absence of approval by such authority, by the European Commission; or

(2) (A) standard contractual clauses approved by the Data Protection Agencies of the Latam Countries or, in the absence of such approval, by the European Commission, are in place between the Cargill Affiliate that is the Data Exporter and Supplier as the Data Importer for the transfer of Personal Information to Processors in countries outside the scope of the Data Protection Laws of the Latam Countries (the Standard Contractual Clauses); and (B) each such contract is filed with the appropriate regulatory authority where required.

In the event that Supplier relies on a legal basis for transferring Personal Information and such legal basis is invalidated (e.g., by a court or competent authority), Cargill shall have the right to suspend all data transfers and Supplier shall cooperate in good faith with Cargill to find an alternative legal basis.

If Supplier deems it necessary to process Personal Information in a manner different from that specified above as a result of applicable laws or regulations in the Latam Countries, Supplier will notify Cargill in writing prior to such processing, unless such notification is prohibited by law for reasons of public interest. Supplier will not perform its obligations under this Agreement in a manner that would cause Cargill to be in breach of its obligations under the Data Protection Laws of the Latam Countries.

For transfers involving Brazilian Personal Information, the Processing of which is subject to Brazil's LGPD, the additional clauses in **Appendix A** will apply.

15. **California Requirements.** Supplier acknowledges and agrees that Cargill has engaged Supplier as a "service provider" (as defined in the CCPA) and has provided any Personal Information of California "consumers" (as defined in the CCPA) to Supplier under the Agreement for a "business purpose" (as defined in the CCPA). To the extent the Processing of Personal Information within the scope of this DPA is subject to the CCPA, the provisions of this Clause 14 shall apply. Supplier: (1) shall at all times comply with the CCPA, including by providing no less than the level of privacy protection as required by the CCPA; (2) shall not retain, use, disclose or otherwise Process Personal Information except as necessary for the business purposes specified in the Agreement or this DPA; (3) shall not "sell" or "share" Personal Information as those terms are defined under the CCPA; (4) shall not combine any Personal Information with Personal Information that Supplier receives from or on behalf of any other third party or collects from Supplier's own interactions with Data Subjects who reside in California, provided that Supplier may so combine Personal Information for a purpose permitted under the CCPA if directed to do so by Cargill or as otherwise expressly permitted by the CCPA; (5) shall promptly notify Cargill if Supplier can no longer comply with the CCPA or its obligations under the Agreement or this DPA, no later than five business days after Supplier makes a determination that it can no longer meet its obligations; and (6) agrees to refrain from taking any action that would cause any transfers of Personal Information to or from Cargill to qualify as "selling" or "sharing" Personal Information. Cargill may, upon providing reasonable notice to Supplier, take all reasonable and appropriate steps to prevent, stop, or remediate any unauthorized Processing of Personal Information.

Cargill EUDR Data Privacy Terms and Conditions

APPENDIX A – TRANSFER CLAUSES

"Transfer Clauses" means Module Two of the Standard Contractual Clauses for Controller-to-Processor transfers approved by EC Decision of 4 June 2021. For purposes of the Transfer Clauses, Cargill is the Data Exporter and Supplier is the Data Importer, and the following provisions shall apply: (1) the parties' execution of this DPA shall be considered as signature to the Transfer Clauses; (2) Supplier agrees to observe the terms of the Transfer Clauses without modification, except as set out in this DPA; (3) neither **Clause 7** (optional docking clause) nor the optional independent dispute resolution provision within **Clause 11(a)** of the Transfer Clauses are used; (4) Option 2 (General Written Authorization) is selected for **Clause 9(a)** of the Transfer Clauses, with respect to the use of sub-processors, with a specific time period of thirty (30) days; (5) with respect to **Clause 12(a)** of the Transfer Clauses, the parties agree that (i) liability between the parties as contemplated in **Clause 12(a)** shall be determined by any liability and/or indemnification provisions in the Agreement; (ii) nothing in **Clause 12(a)** shall change the interpretation of such liability and/or indemnification provisions in the Agreement; and (iii) notwithstanding this Clause of Appendix A, each party remains liable to the Data Subject as contemplated in **Clause 12** of the Transfer Clauses; (6) with respect to **Clause 17** of the Transfer Clauses, if the Agreement is not governed by EU Member State law, the Transfer Clauses will be governed by the law where the Data Exporter is established, unless the Data Exporter is not located in an EU Member State, in which case the Transfer Clauses will be governed by the laws of the Netherlands; (7) with respect to **Clause 18(b)** of the Transfer Clauses, if the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with the Agreement, the parties agree that the courts of the Netherlands shall have exclusive jurisdiction to resolve any dispute arising from the Transfer Clauses.

Appendices B, C and **D** shall also form respective Annexes I, II and III to the Transfer Clauses; (1) if so required by the laws or regulatory procedures of any jurisdiction, the parties shall execute or re-execute the Transfer Clauses as separate documents setting out the proposed transfers of Personal Information in such manner as may be required; and (2) in the event the Transfer Clauses are amended, replaced, or repealed by the European Commission or under Data Protection Laws, the Parties agree to work in good faith to enter into any updated version of the Transfer Clauses or negotiate in good faith a solution to enable a transfer of Personal Information to be conducted in compliance with Data Protection Laws.

Switzerland. In the case of a transfer of Personal Information, the Processing of which is subject to Swiss Data Protection Laws, to a Third Country (either directly or via onward transfer), unless another valid mechanism for the lawful transfer of Personal Information recognized under applicable Data Protection Laws applies (as set forth in Clause 11 of the DPA), the following additional provisions shall apply: (1) any references to the "Clauses" in the Transfer Clauses shall include the amendments set out in this Clause of **Appendix A**; (2) references to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "FADP" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of the FADP; (3) references to "Regulation (EU) 2018/1725" are removed; (4) references to the "Union", "EU" and "EU Member State" are all replaced with "Switzerland"; (5) the footnotes to the Transfer Clauses do not apply; (6) Clause 13(a) and Part C of Annex I of the Transfer Clauses are not used, and the competent supervisory authority is the Switzerland Federal Data Protection and Information Commissioner; and (7) the Transfer Clauses shall be understood to also protect the Personal Information of legal entities until the entry into force of the revised FADP.

UK. In the case of a transfer of Personal Information, the Processing of which is subject to UK Data Protection Laws, to a Third Country (either directly or via onward transfer), unless another valid mechanism for the lawful transfer of Personal Information recognized under applicable Data Protection Laws applies (as set forth in Clause 11 of the DPA), the following additional provisions shall apply: (1) Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses; (2) with respect to Section 19 of the Approved Addendum, in the event the Approved Addendum changes, neither party may terminate the Addendum except as provided for in the Agreement; and (3) any references to the "Clauses" in the Transfer Clauses shall include the amendments set out in this Clause of **Appendix A**.

Additional Transfer Clauses:

Australia. The following provisions apply to all transfers of Personal Information controlled by Data Exporter in Australia: (1) when collecting, using, disclosing and storing Personal Information provided by or on behalf of the Data Exporter, the Data Importer must comply with the Australian Privacy Principles; (2) to the extent Data Importer discloses Personal Information to a third party, Data Importer shall enter into an agreement with such third party that contains terms no less stringent than those described under this DPA.

Brazil. With respect to transfers involving Personal Information whose processing is subject to the Brazilian Law on the Protection of Personal Information (LGPD), the following provisions shall apply: (1) the Data Exporter shall process the Personal Information in compliance with the LGPD and shall only provide instructions to the Data Importer for the processing of such Personal Information that comply with the LGPD; (2) the Data Importer shall carry out the processing of the Personal Information in accordance with the instructions provided by the Data Exporter or as otherwise permitted by applicable law; (3) the Data Exporter shall transfer Personal Information out of Brazil in compliance with Chapter V of the LGPD; and (4) the standard contractual clauses contained in Annex II of Regulation CD/ANPD Nº 019, issued by the Brazilian National Data Protection Agency (ANPD) on August 23, 2024 ("**Brazil Transfer Clauses**") are hereby incorporated into this DPA by reference, and the parties agree that the transfer of Personal Information outside of Brazil shall be governed by such Brazil Transfer Clauses, as amended or replaced from time to time. For purposes of the Brazil Transfer Clauses, both parties agree that: (i) the Data Importer shall not engage in onward transfers of Personal Information; (ii) the Data Exporter shall be responsible for posting on its website a document containing information about the international data transfer, including its purpose, duration, and the rights of the Data Subjects; (iii) the Data Exporter shall be responsible for responding to requests from Data Subjects regarding their Personal Information, such as requests for access, correction, and deletion; (iv) The Data Exporter shall be responsible for notifying the ANPD and the Data Subjects within three (3) working days of any security incident that may pose a risk to the Data Subjects; (v) The security measures to be implemented to protect internationally transferred Personal Information, including specific measures to protect sensitive data and data about children and adolescents, and will at a minimum comply with the security requirements in the attached **Appendix C**.

China. For transfers involving Personal Information, the Processing of which is subject to Data Protection Laws in China: (1) Personal Information shall mean Customer and Supplier Data and Worker Data that is "personal data" or "important data" within the meaning of Chinese Data Protection Laws; (2) Data Exporter will not transfer Personal Information to a place outside of China to the extent that doing so would be prohibited by Chinese Data Protection Laws; (3) Data Exporter shall obtain any and all necessary consents under Chinese Data Protection Laws and meet any other requirements under Chinese Data Protection Laws for lawful transfers of Personal Information to a place outside of China; (4) Data Exporter warrants and undertakes that Personal Information have been collected, Processed and stored in accordance with the laws applicable to Data Exporter in China; (5) in the case of a transfer of Personal Information from Data Exporter to a territory outside China, it is the responsibility of Data Exporter to ensure that the transfer is lawful and data subjects have given their unambiguous consent to the transfer; (6) Data Importer shall Process and use Personal Information received for purposes as consented to by data subjects or as otherwise permitted under Chinese Data Protection Laws; (7) Data Importer shall maintain the security and confidentiality of Personal Information; (8) Data Importer shall avoid providing or transferring the Personal Information to any third party, except when authorized by Data Exporter and consented to by data

subjects (including to subcontractors subject to the same obligations as Data Importer) or when required by applicable law (e.g., when lawfully requested by competent authorities); (9) Data Importer shall update Personal Information according to any instructions from Data Exporter; (10) Data Importer shall make Personal Information accessible to Data Exporter upon reasonable request and provide Data Exporter with information concerning Data Importer's security controls from time to time upon request; and (11) if the Cyberspace Administration of China or other competent government authority issues standard contractual clauses to legitimize the transfer of Personal Information outside of China ("**China Transfer Clauses**"), at such time the China Transfer Clauses are hereby incorporated into this DPA by reference and the Parties agree that the transfer of Personal Information outside of China shall be governed by such China Transfer Clauses as amended or replaced from time to time.

Russia. For transfers of Personal Information, the Processing of which is subject to Data Protection Laws in Russia: (1) Personal Information (Data) shall mean - any information related directly or indirectly to a certain or identifiable physical person (individual). (2) Data Exporter shall obtain any and all necessary consents under Russian Data Protection Laws and meet any other requirements under Russian Data Protection Laws for lawful transfers of Personal Information to a place outside of Russia; (3) when collecting personal data, including using the information and telecommunication network called the internet, data operators shall ensure the recording, systematization, accumulation, storage, clarification (updating, modification), extraction of personal data of the citizens of the Russian Federation using databases located within the territory of the Russian Federation; (4) in the case of a transfer of Personal Information from Data Exporter to a territory outside Russia, it is the responsibility of Data Exporter to ensure:

- that the transfer is lawful and data subjects have given their unambiguous consent to the transfer;

- the database where the Personal data should be initially recorded into, as well as stored and updated at a later stage, must be located in Russia ("primary database"). After that, information from such "primary databases" can be transferred to databases located outside of Russia ("secondary databases"); and

- the recording, systematization, accumulation, storage, clarification (updating, modification), extraction of personal data of the citizens of the Russian Federation using databases located within the territory of the Russian Federation.

(5) Data Importer shall Process and use Personal Information received for purposes as consented to by data subjects or as otherwise permitted under Russian Data Protection Laws; (6) Data Importer shall maintain the security and confidentiality of Personal Information; (7) Data Importer shall avoid providing or transferring the Personal Information to any third party, except when authorized by Data Exporter and consented to by data subjects (including to subcontractors subject to the same obligations as Data Importer) or when required by applicable law (e.g., when lawfully requested by competent authorities); (8) Data Importer shall update Personal Information according to any instructions from Data Exporter; (9) Data Importer shall make Personal Information accessible to Data Exporter upon reasonable request and provide Data Exporter with information concerning Data Importer's security controls from time to time upon request.

Cargill EUDR Data Privacy Terms and Conditions

APPENDIX B – DESCRIPTION OF THE TRANSFER

A. LIST OF PARTIES

Data exporter(s): Cargill

Contact: Data protection enquiries can be addressed by e-mail to Global Privacy Office at privacy@cargill.com.

Role (controller/processor): Data Controller

Data importer(s): Supplier

Role: Data Processor

Activities relevant to the data transferred under these Clauses: The data importer provides services to the data exporter in accordance with the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subject

Farmers and/or producers and/or their employees in the supply chain.

Categories of personal data

Name, address and email; Polygon or GPS point of production location (farm or concession); product description (including type of product, volume, production date and origin country), data to be provided as evidence of compliance with Art. 3(b) in connection with 2(4) of the EUDR such as, but not limited to e.g. land use or registration details, tax related info.

Sensitive data transferred.

No sensitive Personal Information is intended on being Processed by the Supplier on behalf of Cargill.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous, for the duration of the Agreement.

Nature of the processing and Purpose of the data transfer and further processing

Collecting, accessing, storing, hosting, and erasure or destruction of Personal Information to enable the Supplier to perform its obligations under the Agreement to assist Cargill and Cargill's buyers to comply with the EUDR in accordance with Cargill's instructions.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Agreement or for a duration of 6 years, whichever is longer, unless otherwise set out under this DPA or as agreed by the parties in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Any sub-processor must be agreed separately in writing between the parties.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

With respect to Clause 13(a) of the Transfer Clauses: (1) where the Data Exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance with GDPR as regards the data transfer shall act as the competent supervisory authority with respect to Personal Information subject to this DPA; (2) where the Data Exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to GDPR Article 27(1), the supervisory authority of the Netherlands shall act as the competent authority with respect to Personal Information subject to this DPA; and (3) where the Data Exporter is not established in an EU Member State, but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without having to appoint a representative pursuant to Article 27(1), the Netherlands shall act as the competent supervisory authority with respect to Personal Information subject to this DPA.

APPENDIX C - TECHNICAL AND ORGANISATIONAL MEASURES

INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organizational security measures shall include those set out in the Agreement between the parties, as well as those described below. In the event of a conflict between the Agreement, or those described in this Appendix C, the more stringent terms and conditions shall prevail.

Supplier must comply with the following minimum security requirements:

1	Inventory	Maintain an accurate and up to date inventory of systems connected to and software running on your network.
2	Configuration Management	Consistently apply and manage secure configurations on your systems, applications and network devices and have mechanisms to detect and correct configuration drift.
3	Vulnerability Management	Perform at least monthly vulnerability scans and remediate critical and high vulnerabilities within thirty days of discovery? (Critical and high refer to ratings defined by CVSS. Remediate means to mitigate the risk by patching, adjusting configurations or other appropriate actions.)
4	Malware Protection	Have malware defense mechanisms in place that are deployed on all your computing devices and are configured to perform at least weekly scans and to get daily and automatic file definition updates from a trusted source.
5	Life Cycle	All running versions of operating systems, virtualization, networking, middleware, databases and application software in your environment are supported by the corresponding vendor.
6	Patching	Apply high severity security patches within 30 days of release and all other security patches within 90 days, where patch priorities are based on Common Vulnerability Scoring System (CVSS) ratings, or some other rating system? (High severity refer to Critical and Important patch ratings as defined by industry leaders like Microsoft, Red Hat, etc.)
7	Backups	Have processes and tools used to properly back up customer information or services, protect the backups against tampering and a proven methodology for the timely recovery of information or services.
8	Access Control	Use processes and tools to track/control/prevent/correct the use, assignment and configuration of administrative privileges on computers, networks and applications.
9	Networks	Use mechanisms to segregate and protect internal networks from untrusted networks.
10	Centralized Logging	Have mechanisms to collect, manage and analyze event audit logs to help in detecting, understanding and recovering from an attack.