Cargill Data Transfer Addendum

1. **Scope of Applicability.** This Data Transfer Addendum ("**DTA**") is part of Cargill's comprehensive privacy program and shall apply to Personal Information exchanged between the parties in connection with performance of the Agreement and/or any applicable services. In the event of any conflict or inconsistency between the terms of the Agreement and this DTA, the terms of the DTA shall prevail. A Description of the Transfer, a template of which is attached hereto, and a Technical and Organization Measures, a template of which is attached hereto, outlining the specific data and other information covered herein must be provided to Cargill and will be incorporated into this DPA and the Agreement.

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 DTA (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 DTA (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 Breach"** means any (1) compromise of the security, confidentiality, or integrity of Personal Information or Supplier's systems or networks used to secure, protect, or Process Personal Information; (2) unauthorized access to or acquisition, or unauthorized or unlawful Processing of, Personal Information; (3) unauthorized intrusion into, access to, or control, modification, or use of any system or network used by Supplier or one of its Processors (including its Processors' sub-processors) to secure, protect, or Process Personal Information; or (4) event which leads Supplier to suspect, or would lead a reasonable person exercising an appropriate level of diligence and investigation to suspect, that (1), (2), or (3) has occurred; **"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 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 one party to the other party in connection with the performance of 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**," and "**Data Processor,**" 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, each party acts as an independent Data Controller of Personal Data. The parties individually determine the purposes and means of their respective Processing. The parties do not jointly determine the purposes and means of Processing and are thus not joint Controllers in the meaning of Art. 26 of EU GDPR and UK GDPR, as applicable. Each party is responsible for processing Personal Data within the scope of the Agreement and this DTA in accordance with Data Protection Laws.

4. **Description of Data Processing.** The subject matter of the Processing is the performance of the Agreement, and the Processing will be carried out for the duration of the Agreement. Appendices B and C to this DTA, 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 DTA.

5. **Data Security.** It is the responsibility of each party to Process Personal Information within the scope of this DTA in compliance with Data Protection Laws, including, to the extent applicable, Art. 32 of GDPR and analogous provisions under Data Protection Laws. Each party will implement appropriate technical and organizational measures to provide an appropriate and reasonable level of data security.

6. **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 6 of the DTA. To the extent the party that discloses or otherwise makes available Deidentified Data ("**Disclosing Party**") to the other party ("**Receiving Party**"), Receiving Party 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 Receiving Party 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 6 of the DTA (including imposing this requirement on any further Recipients).

7. **Assistance.** The parties will assist each other to the extent reasonably appropriate in complying with requests, queries, or complaints of Data Subjects or supervisory authorities regarding compliance with Data Protection Laws in connection with the DTA. The parties will notice each other of any Data Subject requests relating to Personal Information Processed in connection with the DTA that they receive in accordance with their respective obligations under Data Protection Laws..

8. **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, 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 , the transfer of Personal Information under this DTA shall be governed by that mechanism.

9. **Personal Information from Other Jurisdictions**. To the extent the performance of the Agreement 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, the parties shall (i) cooperate to execute any agreements and to implement all processes and measures necessary 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.

10. **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.

11. **California Requirements.** To the extent either party's disclosure of Personal Information to the other party is considered a "sale" or "sharing" as those terms are defined under the CCPA, this Clause 11 shall apply to Receiving Party's Processing of such Personal Information. In such case, Receiving Party agrees to comply with applicable provisions of the CCPA and apply the same level of privacy protection as required of Disclosing Party under the CCPA with respect to the Processing of such Personal Information. The parties agree that: (1) Disclosing Party has sold or shared Personal Information of California "consumers" (as defined in the CCPA) to Receiving Party under the Agreement only for the limited and specified purposes described in Appendices B and C to this DTA; (2) Disclosing Party may take reasonable and appropriate steps to help to ensure that Receiving Party uses and discloses such Personal Information in a manner consistent with Disclosing Party's obligations under the CCPA; (3) with respect to Receiving Party's Processing of such Personal Information, Receiving Party shall promptly notify Disclosing Party if Receiving Party makes a determination that it can no longer comply with the CCPA; (4) Disclosing Party may, upon providing reasonable notice to Receiving Party, take reasonable and appropriate steps to stop and remediate any unauthorized Processing of such Personal Information.

12. **Breach Notification.** If Supplier becomes aware of any Data Breach, Supplier will: (1) promptly (but in any event within forty-eight (48) hours) report such Data Breach to Cargill, including a description of the nature and anticipated consequences of the Data Breach; (2) mitigate, to the extent practicable, any harmful effects of such Data Breach; and (3) cooperate with Cargill in providing any notices and coordinate any public statements. Supplier will bear (1) the costs incurred by Supplier in complying with its obligations under this Agreement, and (2) in addition to any other damages for which Supplier may be liable for under this Agreement.

Cargill Data Transfer Addendum

APPENDIX A – TRANSFER CLAUSES

"Transfer Clauses" means Module One of the Standard Contractual Clauses for Controller-to-Controller transfers approved by EC Decision of 4 June 2021. For purposes of the Transfer Clauses, Disclosing Party is the Data Exporter and Receiving Party is the Data Importer, and the following provisions shall apply: (1) the parties' execution of this DTA shall be considered as signature to the Transfer Clauses; (2) Receiving Party agrees to observe the terms of the Transfer Clauses without modification, except as set out in this DTA; (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) 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; (5) 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; (6) 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 and C shall also form respective Annexes I and II 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 DTA), 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 DTA), 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 DTA.

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 – if applicable - 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 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**.

Latin America. To the extent that parties process any Personal Information provided by the other party, subject to the data protection laws of Argentina, Colombia, Peru and/or Uruguay ("Latam Countries" or individually "Latam Country"), the parties agree to the following:

With respect to transfers involving Personal Information whose processing is subject to the data protection laws of the Latam Countries, the following provisions shall apply:

1. The Data Exporter shall process the Personal Data in compliance with the applicable data protection laws of Argentina (Law No. 25,326), Colombia (Law No. 1,581), Peru (Law No. 29,733), and Uruguay (Law No. 18,331) and, if applicable, shall only provide instructions to the Data Importer for the processing of such Personal Information that comply with these laws.
2. The Data Importer shall carry out the processing of the Personal Information as permitted by applicable law.
3. The Data Exporter shall transfer Personal Information out of Argentina, Colombia, Peru, or Uruguay to non-adequate jurisdictions in compliance with the relevant provisions of their respective data protection laws.
4. The Standard Contractual Clauses contained in the Implementation Guide on Model Contract Clauses for International Personal Data Transfers (IPDT) published by the Permanent Secretariat of the Ibero-American Data Protection Network (RIPD), in particular the Model Agreement for the International Transfer of Personal Data from Controllers to Controllers, are hereby incorporated by reference into this DPA, and the parties agree that the transfer of personal data outside these countries to non-adequate jurisdictions shall be governed by such Standard Contractual Clauses, as amended or replaced from time to time.

China. For transfers involving Personal Information, the Processing of which is subject to Chinese Data Protection Laws: (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 DTA 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 Information 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 Data Transfer Addendum

APPENDIX B – DESCRIPTION OF THE TRANSFER

EXAMPLE

A. LIST OF PARTIES

Data exporter(s) and Data importer(s):

Name: Cargill, Incorporated

Address: 15407 McGinty Road West, Wayzata, Minnesota 55391-2399.

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

Role (controller/processor): Data Controller

Name: _____

Address: _____

Data protection enquiries can be addressed to _____.

Role (controller/processor): Data Controller

Activities relevant to the data transferred under these Clauses: The parties provide services in accordance with the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

……

Categories of personal data transferred

……

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive Personal Data is intended to be transferred to the Data Importer by the Data Exporter.

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

Collecting, accessing, storing, hosting, and erasure or destruction of Personal Data to enable the Parties to perform their obligations under the Agreement.

Purpose(s) of the data transfer and further processing

Collecting, accessing, storing, hosting, and erasure or destruction of Personal Information to enable the Parties to perform their obligations under the Agreement.

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 unless otherwise set out under this DTA or as agreed by the parties in writing.

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

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 DTA; (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 DTA; 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 DTA.

APPENDIX C - TECHNICAL AND ORGANISATIONAL MEASURES

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

EXAMPLE

EXPLANATORY NOTE:

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

Technical and organizational measures shall be implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. These measures shall apply to any transfers to (sub-) processors as well.

Examples of possible measures:

Measures of pseudonymization and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Measures for user identification and authorization

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimization

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]