DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the Marco Technologies Relationship Agreement ("**Principal Agreement**") dated _____ between: (i) Marco Technologies, LLC ("**Marco**") acting on its own behalf and, as applicable, as agent for each Marco Affiliate; and (ii) _____ ("**Company**") acting on its own behalf and, as applicable, as agent for each Company Affiliate (collectively, "**Company Group Member**").

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1. "**Applicable Law(s)**" means any applicable national, federal, state, provincial, local, and other laws, regulations, industry-recognized codes of conduct or other legal requirements governing the relationship between Marco or Marco Affiliates and Company or Company Affiliates and the Services provided under the Principal Agreement, including but not limited to, as applicable, laws governing the privacy and security of personally identifiable information, including the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"), the Personal Information Protection Law of China ("PIPL"), the General Law for the Protection of Personal Data13709/2018 in Brazil ("LGPD"), the California Consumer Protection Act, as amended by the California Privacy Rights Act (Cal. Civ. Code 1798.100 – 1798.199) ("CCPA"), the Colorado Privacy Act (Colo. Rev. Stat. §§ 6-1-1301–13), the Connecticut Data Privacy Act of 2022, the Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101–404), and the Virginia Consumer Data Protection Act (Va. Code Ann. §§ 59.1-575–85) (collectively the "Data Protection Laws") and any laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time.

1.1.2. "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3. "**Company Group Member**" means Company or any Company Affiliate;

1.1.4. "**Company Personal Data**" means (a) all individually identifiable information created, collected, accessed, received or otherwise Processed; and (b) any other information that Applicable Law treats as "personal information" (or equivalent term, including without limitation, "personal data," "personally identifiable information," and "nonpublic personal

information") Processed by a Contracted Processor for or on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.5. "**Contracted Processor**" means Marco, Marco Affiliate, or a Subprocessor;

1.1.6. "**Data Protection Losses**" means all liabilities, including all:

1.1.6.1. costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

1.1.6.2. to the extent permitted by Applicable Law:

a. administrative fines, penalties, sanctions, liabilities or other remedies imposed by a regulatory authority;
b. compensation which is ordered by a regulatory authority to be paid to a Data Subject; and
c. the reasonable costs of compliance with investigations by a regulatory authority;

but excluding:

any loss of actual or anticipated income or profits; loss of contracts; loss of goodwill or reputation; loss for any special, indirect or consequential loss or damage of any kind howsoever arising and whether caused by tort (including negligence), breach of contract or otherwise, whether or not such loss or damage is foreseeable, foreseen or known.

1.1.7. "**EEA**" means the European Economic Area;

1.1.8. "**Restricted Transfer**" means:

1.1.8.1. a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.8.2. an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Applicable Law (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Law) in the absence of the Standard Contractual Clauses set forth in Annex 4 below or use of other valid transfer mechanism permitted under Data Protection Laws;

1.1.9. "**Services**" means the products or services Marco provides to Company under the Principal Agreement;

1.1.10. "**Standard Contractual Clauses**" means the agreement pursuant to the European Commission's Implementing Decision of 4.6.2021 on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council dated June 4, 2021, and any replacement, amendment or restatement of the foregoing issued by the European Commission, the current form of which is set out in Annex 4;

1.1.11. "**Subprocessor**" means any party (including any third party and any Marco Affiliate) engaged directly or indirectly by Marco to Process Company Personal Data of any Company Group Member pursuant to the Principal Agreement and this Addendum; and

1.1.12. "**Marco Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Marco, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2. The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR or other applicable Data Protection Laws, and their cognate terms shall be construed accordingly. The term "**Service Provider**" shall have the same meaning as in the CCPA.

1.3. The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Roles and Authority

2.1. The parties agree that, for the Company Personal Data, the Company shall be the data controller and Marco and any Marco Affiliate shall be the data processor(s) as defined under the GDPR.

2.2. The parties agree that, for the Company Personal Data, the Company is a "business" and Marco and any Marco Affiliate are "service providers" as defined under the CCPA.

2.3. Marco and Marco Affiliates shall process Company Personal Data in compliance with the terms of this Addendum and Applicable Law. As applicable, Marco warrants and represents that, before any Marco Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Marco's entry into this Addendum as agent for and on behalf of that Marco Affiliate will have been duly and effectively authorized, or subsequently ratified, by that Marco Affiliate.

2.4. The Company and any Company Affiliate shall comply with Applicable Law and the terms of this Addendum in providing any Company Personal Data to any Contracted Processors. The Company warrants, represents and undertakes, that:

2.4.1. All Company Personal Data, shall comply in all respects, including in terms of its collection, storage and processing with Applicable Laws, (which shall include the Company providing all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects); and

2.4.2. All instructions given by it to Contracted Processors in respect of Company Personal Data shall at all times be in accordance with Applicable Laws.

2.4.3. The Company shall not unreasonably withhold, delay or condition its agreement to any change requested by any Contracted Processor in order to ensure the Services and each Contracted Processor can comply with Applicable Law.

2.4.4. The company agrees that:

2.4.4.1. it shall be the responsibility of the Company to provide all necessary wording, notices and policies ("Privacy Notices") in respect of the acquisition of that Company Personal Data for use by the Contracted Processor in the delivery of the Services to ensure

compliance with all Applicable Laws governing both the acquisition of that Company Personal Data and subsequent use thereof by the Company and Marco, and the Privacy Notices shall include without limitation all and any necessary consent requests, privacy statements and privacy policies of the Company and

2.4.4.2. the Contracted Processors shall not be liable for any loss, delay or prejudice of any kind caused by the Company's failure to supply any reasonably requested Privacy Notices in a timely manner or otherwise comply with the Data Subject notice, choice and consent requirements of Applicable Law.

3. Data Processing Instructions for Company Personal Data

3.1. Marco and Marco Affiliate shall:

3.1.1. Process the Company Personal Data (i) on written instructions from any Company Group Member, as further specified in this Addendum, or (ii) where required to do so under Applicable Law to which Marco or Marco Affiliate is subject;

3.1.2. ensure that persons authorized by Marco, and any Marco Affiliate, to Process the Company Personal Data have committed themselves to confidentiality or are under an appropriate statutory or contractual obligation of confidentiality;

3.1.3. take all applicable measures required of Marco, or Marco Affiliates, as a Processor pursuant to Article 32 of the GDPR and other Applicable Law, as further specified in Section 5 of this Addendum;

3.1.4. comply with the conditions referred to in Section 6 of this Addendum for engaging another Processor of Company Personal Data to provide the Services;

3.1.5. provide each Company Group Member reasonable assistance in the fulfilment of any obligations to respond to Data Subject requests, as applicable, and required by Applicable Law;

3.1.6. assist any Company Group Member, at Contracted Processor's then-current hourly rates, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR and other Applicable Law, taking into account the nature of Processing and the information available to Company;

3.1.7. return or provide an opportunity for any applicable Company Group Member to retrieve or otherwise securely delete all Company Personal Data after the end of the provision of Services. At a Company Group Member's request, Marco or Marco Affiliate shall delete Company Personal Data except for (i) secure back-ups deleted in the ordinary course of business according to an established data retention policy, and (ii) Company Personal Data for which retention is required by Applicable Law; in the event of either (i) or (ii), Marco will provide notice of such required retention to the requesting Company Group Member and continue to comply with the relevant provisions of this Addendum with respect to such retained Company Personal Data until such Company Personal Data has been deleted;

3.1.8. make available to any requesting Company Group Member information necessary to demonstrate compliance with this Addendum and Applicable Law;

3.1.9. inform Company Group Member if it makes a determination that it can no longer meet its

obligations under this Addendum or if, in Marco's opinion, any written instruction from Company infringes Applicable Law; and

3.1.10. inform Company Group Member of and provide reasonable assistance in meeting Company's obligations in regard to any Personal Data Breach, in accordance with Section 8 below.

3.2. Service Provider Processing Instructions:

3.2.1. As a Service Provider, and when applicable, Marco and Marco Affiliates shall not:

3.2.1.1. sell, share, rent, release, disclose, disseminate, make available, transfer or otherwise communicate the Company Personal Data to a third party for monetary or other valuable consideration;

3.2.1.2. retain, use, or disclose Company Personal Data outside of the business relationship between the parties or for purposes other than the performance of the Services, unless otherwise stated by Applicable Law; or

3.2.1.3. combine Company Personal Data that Service Provider receives from, or on behalf of, the Company Group Member with any personal data that it receives from, or on behalf of, another person or business or any personal data that Service Provider collects from its own interaction with customers, unless otherwise stated by Applicable Law.

3.3. Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by Article 28(3) of the GDPR and, possibly, equivalent requirements of other Applicable Law. Company may make reasonable amendments to Annex 1 by written notice to Marco from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 confers any right or imposes any obligation on any party to this Addendum.

4. Marco and Marco Affiliate Personnel

Marco and each Marco Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, and ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Technical and Organizational Controls and Security

5.1. Marco shall maintain the technical and organizational controls and security measures for the protection of Company Personal Data as set forth in this Addendum in Annex 2. Marco may update its security practices provided that the measures provided during any term of Service shall in no event provide less protection than those included as of the effective date of such term.

6. Subprocessing

6.1. Subject to the terms of this Section 6, Company and Company Affiliate consent to Marco and Marco Affiliates engaging Subprocessors for the Processing of Company Personal Data.

6.2. Marco shall inform the Company of any intended changes concerning the addition or replacement of Subprocessors. If the Company subsequently objects to the use and appointment of any

Subprocessor by Marco or Marco Affiliate, the Company shall notify Marco immediately in writing. Marco shall have the right to terminate the Principal Agreement with immediate effect to the extent that it relates to the services which require the use of the proposed Subprocessor.

6.3. With respect to each Subprocessor, Marco or the relevant Marco Affiliate shall:

6.3.1. carry out reasonable due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement and this Addendum;

6.3.2. ensure that Subprocessors are bound by written agreements that require them to provide at least the level of Company Personal Data protection required by this Addendum.

7. Assistance with Data Subject Requests

7.1. Marco and Marco Affiliates shall:

7.1.1. promptly notify Company if any Contracted Processor receives a request from a Data Subject and shall redirect the Data Subject to make its request directly to applicable Company Group Member; and

7.1.2. ensure that the Contracted Processor does not respond to that request except on the documented instructions of the applicable Company Group Member or as required by Applicable Law to which the Contracted Processor is subject, in which case Marco shall to the extent permitted by Applicable Law inform Company of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1. Marco shall notify Company without undue delay upon any Contracted Processor becoming aware of a Personal Data Breach, as defined under Applicable Law, affecting Company Personal Data in any Contracted Processor's possession or under its control, providing Company with sufficient information, to the extent available to Marco, to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Applicable Law.

8.2. Marco shall cooperate with Company and any applicable Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Marco and each Marco Affiliate shall, at their then-current hourly rates, provide reasonable assistance to each applicable Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by Article 35 or 36 of the GDPR or equivalent provisions of any other Applicable Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, Contracted Processors.

10. Audit Rights

10.1. Company may carry out appropriate audits, at Company's own expense, of Marco's or Marco Affiliate's Processing of Company Personal Data as required by Applicable Law. Any such audit shall be conducted during normal business hours at agreed dates and times, without disruption to Marco's or Marco Affiliate's business and in accordance with Marco's security rules and requirements, and with a minimum of 60 days written notice to Marco.

10.2. Prior to any audit, Marco and each Marco Affiliate undertakes to provide to each Company Group Member all reasonably requested information and evidence to demonstrate compliance with this Addendum, and Company shall review this information prior to undertaking any independent audit.

10.3. Information and audit rights of the Company Group Members only arise under Section 10.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Applicable Law (including, where applicable, Article 28 of the GDPR).

10.4. A Company Group Member may use a third-party auditor for such audits with Marco's or Marco Affiliate's agreement. Marco or any relevant Marco Affiliate shall not unreasonably withhold or delay agreement to the addition of a new auditor to that list. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with Marco or Marco Affiliate.

11. Restricted Transfers

11.1. Subject to Section 11.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

11.2. The Standard Contractual Clauses shall come into effect under Section 11.1 on the later of:

11.2.1. the data exporter becoming a party to them;

11.2.2. the data importer becoming a party to them; and

11.2.3. commencement of any relevant Restricted Transfer.

11.3. Section 11.1 shall not apply to a cross-border transfer of Company Personal Data unless the cross-border transfer is a Restricted Transfer and Section 11.1, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), allows the relevant Restricted Transfer to take place without breach of Applicable Law.

12. Modifications, Supplementation, Term, Limits of Liability and Indemnity

12.1. Marco or the Company may modify or supplement this Addendum, with notice to the other party, (i) if required to do so by a Supervisory Authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement Standard Contractual Clauses or other transfer mechanism approved under Applicable Law, (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40 and 42 of the GDPR, or (v) to comply with any request or requirement imposed by an applicable third-party data

controller.

12.2. Without prejudice to this Addendum, either party may from time to time provide additional information and detail about how it will execute this Addendum in its product-specific technical, privacy, or policy documentation.

12.3. This Addendum shall be effective on the date the second signature is affixed below and shall expire upon the later of (a) the termination of the Principal Agreement or (b) cessation of any Processing of Company Personal Data by Marco or Marco Affiliate on behalf of the Company Group Member pursuant to the provision of the Services.

12.4. Marco shall be liable for and indemnify, and keep indemnified, any Company Group Member against Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this Addendum:

12.4.1. only to the extent caused by a Contracted Processor's gross negligence or willful misconduct with regard to the Processing by such Contracted Processor of Company Personal Data under this Addendum and directly resulting from Marco's breach of clauses 1 to 12 (inclusive); and

12.4.2. in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any negligence, willful misconduct, or breach of this Addendum by a Company Group Member.

12.5. Any applicable Company Group Member shall be liable for and indemnify, and keep indemnified, any Contracted Processor in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, Marco, Marco Affiliate and any Subprocessor arising from or in connection with any:

12.5.1. non-compliance by the Company with Applicable Law;

12.5.2. processing carried out by any Contracted Processor pursuant to any Processing instruction from a Company Group Member that infringes any Applicable Law; or

12.5.3. breach by any Company Group Members of any of its obligations under this Addendum.

12.6. These Sections 12.4-12.6 are intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Applicable Laws to the contrary, except:

12.6.1. to the extent not permitted by Applicable Law; and

12.6.2. that it does not affect the liability of either party to any Data Subject.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

[Company DBA Name]

Signature _____

Name _____

Title _____

Date Signed _____

Marco Technologies, LLC

Signature _____

Name _____

Title _____

Date Signed _____

ANNEX 1 TO ADDENDUM: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required in Section 3.3 of this Addendum.

Subject matter and duration of the Processing of Company Personal Data
The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data
The nature and purpose of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

The types of Company Personal Data to be Processed
[Include list of data types here]

The categories of Data Subject to whom the Company Personal Data relates
[Include categories of data subjects here]

Processing Operations:
The Company Personal Data will be subject to Processing as detailed in the Principal Agreement and Addendum.

The obligations and rights of Company and Company Affiliates
The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

Sensitive Data
[EXAMPLES

- Racial and ethnic origin;
- Sexual orientation;
- Political opinions;
- Background and cultural identification;
- Trade union membership;
- Religious or other beliefs of a similar nature;
- Biometric or genetic information;
- Physical or mental health or condition;
- Education records;
- Banking or credit account information;
- Financial accounts, applications, or statements;
- Intellectual Property (IP);
- Employment information or trade secrets;
- Information labelled as sensitive/confidential; and
- Criminal offences or proceedings, outcomes and sentences
- If no sensitive data is processed, please write "not applicable"]

ANNEX 2 TO ADDENDUM: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

Marco maintains commercially reasonable and risk-based administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of Company Personal Data. The following provides high-level summary of those safeguards. This is not intended to be an exhaustive list, as Marco continually improves its security position in response to changes in business and emerging threats.

- **Change Management**: Marco maintains logs that document all changes to the information technology operating environment, such as the addition of a server, modifying of code/configurations, or any and all changes affecting production equipment.
- **Encryption:** Marco encrypts all Company data, both at rest and in transit. All Marco backups utilize full Advanced Encryption System ("AES").
- **Information Security Program:** Marco maintains a comprehensive written information security program including administrative, technical, and physical safeguards to protect Company Personal Data.
- **Multi-Factor Authentication:** Marco enforces multi-factor authentication for all users with administrative privileges or elevated accounts.
- **Password Management**: All Marco users are required to use strong passwords and change those passwords on a regular basis. In addition, all passwords for administrative accounts are maintained in a key vault with multi-factor authentication in place.
- **Patch Management:** Marco maintains and pushes critical security updates for all equipment in accordance with Marco patching policies.
- **Physical Safeguards:** All Marco locations and data centers employ an access control system with clearance badges. Regular access reviews take place to ensure least privilege access is maintained in secure Marco facilities.
- **Risk Assessment & Penetration Testing:** Marco performs annual information security risk assessments with penetration testing, as well as quarterly phishing campaigns.
- **Scanning:** Marco performs vulnerability scans of all devices connected to its network by executing real-time anti-virus scans and malware scans, as well as full-time use of intrusion detection and penetration systems. Marco also scans all emails for potentially malicious content and provides Marco users the ability to report and quarantine as desired.
- **Security Policies:** Information security policies, procedures and requirements have been defined, documented, implemented and communicated to internal and external parties responsible for system security.
- **Training & Awareness:** Marco mandates its employees complete annual security awareness training. Incident response training is conducted at least annually with employees responsible for incident response functions. Marco maintains an ongoing awareness program to keep employees apprised of new requirements and threats.

ANNEX 3 TO ADDENDUM: SUBPROCESSOR LIST

All Subprocessors listed in this Annex 3 have been approved and authorized by Company and Company Affiliates.

Subprocessor Info		
Subprocessor Company Name(s) and Address(es) (full legal entity name):	Subprocessor contact person (name, position and contact details):	Description of Processing (including clear delimitation of responsibilities in case several Subprocessors are authorized and including subject matter, nature and duration of the Processing)

ANNEX 4 TO ADDENDUM:
STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization:

[INSERT NAME] (identified as "Company" in the Addendum) and any Company Affiliate

(the data **exporter**)

And

The entity identified as Marco in the Addendum and any Marco Affiliate or authorized Subprocessor (as defined in the Addendum) for whom Marco is authorized as an agent to enter these Standard Contractual Clauses

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in the Appendix.

SECTION I

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

b. The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
ii. Clause 8 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);
iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);
iv. Clause 12 - Module Two: Clause 12(a), (d) and (f);
v. Clause 13;
vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e);
viii. Clause 18 - Module Two: Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking Clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial

notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of Sub-processors

MODULE TWO: Transfer controller to processor

a. GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least *[Specify time period]* in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

- the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data Subject Rights

MODULE TWO: Transfer controller to processor

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to: (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13; (ii) refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws

Clause 12

Liability

MODULE TWO: Transfer controller to processor

a. The data Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

a. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

   [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

   [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];
iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in the case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Instructions

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the

obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   ii. the data importer is in substantial or persistent breach of these Clauses; or
   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679

becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be _____ (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of the Member State in which the data exporter is established.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: The data exporter is the entity identified as "Company" in the Addendum, and each Company Affiliate.

Address:

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: The activities detailed in the Principal Agreement and Addendum.

Signature and date: …

Role (controller/processor): Controller

Data importer(s):

1. Name: The data importer is the entity identified as Marco in the Addendum, or a Marco Affiliate or authorized Subprocessor (as defined in the Addendum) for whom Marco is authorized as an agent to enter these Standard Contractual Clauses.

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: The activities detailed in the Principal Agreement and Addendum.

Signature and date: …
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred.

The personal data transferred concern the categories of data subjects set forth in Annex 1 of the Addendum under the header "The categories of Data Subject to whom the Company Personal Data relates."

Categories of personal data transferred.

The personal data transferred concern the categories of personal data set forth in Annex 1 of the Addendum under the header "The types of Company Personal Data to be Processed."

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.

The personal data transferred concern the sensitive data set forth in Annex 1 of the Addendum under the header "Sensitive Data."

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

The frequency of the transfer shall be on a continuous basis as necessary to perform the obligations of the Principal Agreement (as defined in the Addendum).

Nature of the processing

The personal data transferred will be subject to the following basic processing activities (please specify): The processing operations are defined in Annex 1 of the Addendum under the heading "The nature and purpose of the Processing of Company Personal Data."

Purpose(s) of the data transfer and further processing

The personal data transferred will be subject to the following basic processing activities (please specify): The processing operations are defined in Annex 1 of the Addendum under the heading "The nature and purpose of the Processing of Company Personal Data."

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

The personal data will be retained solely for as long as necessary to complete any processing necessary to provide the Services under the applicable Principal Agreement (as defined in the Addendum), and as otherwise required by Applicable Law.

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

As set forth in Section 6 of the Addendum and including, without limitation, Annex 3 to the Addendum.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

Where the data exporter is established in an EU Member State, the EU Member State in which the data exporter is established. Where the data exporter is not established in an EU Member State, the EU Member State identified in Clause 17.

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:
The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures 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.

As set forth in Annex 2 of the Addendum and including, without limitation, Section 5 to the Addendum.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

As set forth in Annex 2 of the Addendum and including, without limitation, Section 5 to the Addendum.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

As set forth in Annex 3 of the Addendum and including, without limitation, Section 6 to the Addendum.

