STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS

SECTION I

Clause 1. **Purpose and scope**

a) The purpose of these standard contractual clauses is to ensure that 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 (1) (General Data Protection Regulation) are met for the transfer of personal data to a third country.

b) The parties:
i) the natural or legal person(s), public authority(ies), service(ies) or body(ies) (hereinafter, "entity" or "entities") that will transfer the personal data, listed in Annex I.A (each hereinafter referred to as "data exporter"), and
ii) the entity(ies) in a third country that will receive the personal data from the data exporter directly or indirectly through another entity that is also a party to this specification, listed in Annex I.A (each hereinafter referred to as 'data importer'), have agreed to these standard contractual clauses (hereinafter referred to as 'specification').

c) These specifications apply to the transfer of personal data specified in Annex I.B.

d) The appendix to these specifications, which contains the annexes referred to in these specifications, forms part of the specifications.

Clause 2. **Effect and invariability of the clauses**

a) This specification provides for adequate safeguards, including enforceable rights of data subjects and effective legal remedies, in accordance with Articles 46(1) and 46(2)(c) of Regulation (EU) 2016/679 and, in relation to transfers of data from controllers to processors or from processors to other processors, in accordance with the standard contractual clauses referred to in Article 28(7) of Regulation (EU) 2016/679 provided that they are not modified, except for the purpose of selecting the appropriate module(s) or adding or updating information in the appendix. This does not preclude the parties from including the standard contractual clauses contained in this specification in a wider contract, or from adding any additional clauses or guarantees provided that they do not directly or indirectly contradict this specification or prejudice the fundamental rights or freedoms of data subjects.

b) This specification is without prejudice to the obligations to which the data exporter is subject under Regulation (EU) 2016/679.

Clause 3. **Third party beneficiaries**

a) The interested parties may, as third party beneficiaries, invoke this specification against the exporter and/or the data importer and require them to comply with it, with the following exceptions.

I. Clauses 1, 2, 3, 6 and 7.
II. Clause 8: [Module One] Clause 8.5(e) and Clause 8.9(b); [Module Two] Clause 8.1(b) and Clause 8.9(a), (c), (d) and (e); [Module Three] Clause 8.1(a), (c) and (d) and clause 8.9(a), (c), (d), (e), (f) and (g); [module four] clause 8.1(b) and clause 8.3(b).
III. Clause 9: [module two] clause 9(a), (c), (d) and (e); [module three] clause 9(a), (c), (d) and (e).
IV. Clause 12: [module one] clause 12(a) and (d); [modules two and three] clause 12(a), (d) and (f).
V. Clause 13.

VI. Clause 15.1(c), (d) and (e).
VII. Clause 16(e).
VIII. Clause 18: [modules one, two and three] clause 18(a) and (b); [module four] clause 18.

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

Clause 4. **Interpretation**

a) Where terms defined in Regulation (EU) 2016/679 are used in this specification, they are understood to have the same meaning as in that Regulation.

b) These specifications must be read and interpreted in accordance with the provisions of Regulation (EU) 2016/679.

c) These specifications may not be interpreted in a way that conflicts with the rights and obligations set out in Regulation (EU) 2016/679.

Clause 5. **Hierarchy**

In the event of any inconsistency between these terms and conditions and the provisions of related agreements between the parties in force at the time when these terms and conditions were agreed or came into force, these terms and conditions shall prevail.

Clause 6. **Description of transfer(s)**

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

Clause 7 (optional). **Incorporation clause**

a) Any entity not party to this specification may, with the consent of all parties, accede to this specification at any time, either as a data exporter or as a data importer, by completing the appendix and signing Annex I.A.

b) Upon completion of the Appendix and signature of Annex I.A, the acceding entity shall be considered a party to these specifications and shall have the rights and obligations of a data exporter or a data importer, depending on the category in which it is listed in Annex I.A.

c) The acceding entity shall not acquire any rights and obligations under these terms and conditions arising from the period prior to accession.

SECTION II: OBLIGATIONS OF THE PARTIES

Clause 8. **Data protection safeguards**

The data exporter warrants that it has made reasonable efforts to determine that the data importer can, by applying appropriate technical and organisational measures, meet its obligations under this specification.

8.1. Instructions

a) The data importer shall only process personal data on the basis of 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 such instructions.

8.2. Purpose limitation

The data importer shall process personal data only for the specific purposes of the transfer as set out in Annex I.B, except when following further instructions from the data exporter.

8.3. Transparency

Upon request, the data exporter shall make available to the data subject, free of charge, a copy of this specification, including the appendix completed by the parties. To the extent necessary to protect business secrets or other confidential information, such as the measures described in Annex II and personal data, the data exporter may redact the text of the Addendum to this specification before sharing a copy, but shall provide a meaningful summary if failure to do so would prevent the data subject from understanding the content of the Addendum or exercising its rights. Upon request, the parties shall communicate to the data subject the reasons for the redaction, to the extent possible without disclosing 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 personal data it has received are inaccurate or out of date, it shall inform the data exporter thereof without undue delay. In this case, the data importer shall cooperate with the data exporter to delete or rectify the data.

8.5. Duration of processing and deletion or return of data

The processing by the data importer shall only be carried out for the period specified in Annex I.B. After the processing services have been provided, the data importer shall, at the request of the data exporter, either delete all personal data processed on behalf of the data exporter and provide evidence to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete any existing copies. Until the data are destroyed or returned, the data importer shall continue to ensure compliance with this specification. If the law of the country applicable to the data importer prohibits the return or destruction of personal data, the data importer undertakes to continue to ensure compliance with this specification and shall only process the data to the extent and for the duration required by the law of the country. This is without prejudice to Clause 14 and in particular to the obligation of the data importer under Clause 14 to inform the data exporter throughout the duration of the contract if it has reason to believe that it is or has been subject to regulations or practices that do not comply with the requirements of Clause 14(a).

8.6. Security of treatment

a) The data importer and, during the transfer, also the data exporter shall implement appropriate technical and organisational measures to ensure data security; in particular, protection against security breaches resulting in the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure or access ('personal data breach'). In determining an 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 purposes of the processing, and the risks posed by the processing to the data subjects. The parties shall in particular consider encryption or pseudonymisation, especially during transmission, if the purpose of the processing can be fulfilled in this way. In case of pseudonymisation, the additional information necessary to attribute personal data to a specific data subject should, as far as possible, remain under the sole control of the data exporter. In fulfilling its obligations under this paragraph, the data importer shall implement at least the technical and organisational measures set out in Annex II. The

The data importer shall carry out regular checks to ensure that these measures continue to provide an adequate level of security.

b) The data importer shall grant access to personal data to members of its staff only to the extent strictly necessary for the performance, management and monitoring of the contract. It shall ensure that the persons authorised to process the personal data have undertaken to respect confidentiality or are subject to a confidentiality obligation of a statutory nature.

c) In the event of a breach of security of personal data processed by the data importer pursuant to this specification, the data importer shall take appropriate measures to remedy the breach and, in particular, measures to mitigate the negative effects. The data importer shall also notify the data exporter without undue delay upon becoming aware of the security breach. Such notification shall include details of a contact point from which further information can be obtained, a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and personal data records affected), the likely consequences and the measures taken or proposed to be taken to remedy the security breach, in particular, where appropriate, measures to mitigate its possible adverse effects. Where and to the extent that all information cannot be provided at the same time, the initial notification shall provide the information currently available, and additional information shall be provided without undue delay as it becomes available.

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

8.7. Sensitive data

To the extent that the transfer includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data intended to uniquely identify a natural person, data concerning the health or data concerning the sex life or sexual orientation of a natural person, 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 personal data to a third party on the documented instructions of the data exporter. Moreover, the data may only be disclosed to third parties located outside the European Union (4) (in the same country as the data importer or in another third country; hereinafter 'onward transfer') if the third party is bound by or consents to be bound by this specification, with the choice of the relevant module, or if:

I. the onward transfer is to a country covered by an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 covering the onward transfer;

II. the third party otherwise provides adequate safeguards, within the meaning of Article 46 or 47 of Regulation (EU) 2016/679, in respect of the processing in question;

III. if the onward transfer is necessary for the establishment, exercise or defence of claims in connection with specific administrative, regulatory or judicial proceedings; or

IV. if the onward transfer is necessary to protect the vital interests of the data subject or of another natural person. The validity of onward transfers depends on the data importer providing the other assurances provided for in this specification, and in particular the purpose limitation.

8.9. Documentation and compliance

a) The data importer shall resolve promptly and appropriately any queries from the data exporter related to the processing in accordance with this specification.

b) The parties must be able to demonstrate compliance with this specification. In particular, the data importer shall keep sufficient documentation of the processing activities carried out on behalf of the data exporter.

c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in this specification and, upon request of the data exporter, shall allow and contribute to audits of the processing activities covered by this specification, at reasonable intervals or if there are indications of non-compliance. In deciding whether to conduct 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 itself or to authorise an independent auditor. Audits may take the form of inspections of the data importer's physical premises or facilities and, where appropriate, be carried out with reasonable notice.

e) The parties shall make the information referred to in points (b) and (c), and in particular the results of audits, available to the competent supervisory authority upon request.

Clause 9. **Use of Sub-agents**

a) The Data Importer shall not subcontract any of its processing activities carried out on behalf of the Data Exporter under these Clauses to a Sub-processor without the prior specific written authorisation of the Data Exporter. The data importer shall submit the request for specific authorisation at least thirty (30) calendar days prior to the engagement of the sub-processor, together with the information necessary for the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter is set out in Annex III. The Parties shall keep Annex III up to date.

b) Where the data importer uses a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by means of a written contract setting out, in substance, the same data protection obligations as those imposed on the data importer under this Specification, in particular as regards the rights of data subjects as third party beneficiaries (8). The Parties agree that, by complying with this Specification, the data importer also complies with its obligations under clause
8.8. The data importer shall ensure that the sub-provider complies with its obligations under this specification.

c) The data importer shall provide the data exporter, upon request, with a copy of the contract with the sub-processor and any subsequent amendments thereto. To the extent necessary to protect trade secrets or other confidential information, such as personal data, the data importer may redact the text of the contract before sharing the copy.

d) The data importer shall remain fully liable to the data exporter for the performance of the obligations imposed on the sub-processor by its contract with the data importer. The data importer shall notify the data exporter of any breach by the sub-processor of its obligations under that contract.

e) The data importer shall agree with the sub-processor a third party beneficiary clause whereby, in the event that the data importer de facto disappears, ceases to exist in law or becomes insolvent, the data exporter shall have the right to terminate the sub-processor's contract and order the sub-processor to delete or return the personal data.

Clause 10. **Rights of the data subject**

a) The data importer shall promptly notify the data exporter of requests received from the data subject. It shall not respond to such a 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 when responding to requests to exercise the rights conferred on data subjects by Regulation (EU) 2016/679. In this regard, the parties shall set out in Annex II appropriate technical and organisational measures, taking into account the nature of the processing, ensuring that the controller will be assisted in implementing this clause, as well as the purpose and scope of the assistance required.

c) In fulfilling its obligations under points (a) and (b), the data importer shall follow the instructions of the data exporter.

Clause 11. **Redress**

a) The data importer shall inform data subjects, in a transparent manner and in an easily accessible format, by individual notification or on its website, of the authorised contact point for handling complaints. The data importer shall promptly handle complaints received from data subjects.

   The data importer accepts that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform data subjects, in the manner set out in point (a), of such a redress mechanism and that they are not obliged to use it or to follow any particular sequence in seeking redress.

b) In the event of a dispute between an interested party and one of the Parties concerning the fulfilment of these clauses, that Party shall use its best efforts to resolve the matter amicably in a timely manner. The Parties shall keep each other informed of such disputes and, where appropriate, cooperate to resolve them.

c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the data subject's decision to
   I. lodge a complaint with the supervisory authority of the Member State of his habitual residence or place of work, or with the competent supervisory authority in accordance with Clause 13;
   II. submit the dispute to the competent courts within the meaning of clause 18.

d) The Parties agree that the data subject may be represented by a non-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e) The data importer shall comply with a binding decision under applicable EU or Member State law.

f) The data importer agrees that the choice made by the data subject shall not prejudice his or her substantive and procedural rights to seek remedies in accordance with applicable law.

Clause 12. **Liability**

a) Each Party shall be liable to the other(s) for any damages it causes to the other(s) for breach of these clauses.

b) The data importer shall be liable to the data subject, and the data subject shall be entitled to compensation, for any material or non-material damage caused by the data importer or its sub-agent to the data subject for infringing the rights of third party beneficiaries under these clauses.

c) Notwithstanding point (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to compensation, for any material or non-material damage which the data exporter or the data importer (or its sub-processor) causes to the data subject by infringing the rights of third party beneficiaries 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, the controller's liability 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 subparagraph (c) for damage caused by the data importer (or its sub-agent), it shall be entitled to claim from the data importer that part of the compensation corresponding to the data importer's liability for the damage.

e) Where more than one Party is liable for any damage caused to the data subject as a result of a breach of these clauses, all liable Parties shall be jointly and severally liable and the data subject shall have the right to bring an action against any of these Parties.

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

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

Clause 13. **Monitoring**

a) Where the data exporter is established in a Member State of the EU:]] The supervisory authority responsible for ensuring the compliance of the data exporter with Regulation (EU) 2016/679 with regard to the transfer of data, as referred to in Annex I.C., shall act as the 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 Article 3(2) thereof and has appointed a representative in accordance with 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 referred to in Annex I.C, shall act as the 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 Article 3(2) thereof, without, however, having to appoint a representative in accordance with Article 27(2) of Regulation (EU) 2016/679:]. The competent supervisory authority shall be the supervisory authority of one of the Member States in which the data subjects whose personal data are transferred pursuant to these Clauses in connection with the offering of goods or services to them, or whose behaviour is monitored, as referred to in Annex I.C, are located.

b) The data importer agrees to submit to the jurisdiction of the competent supervisory authority and to cooperate with it in any procedure aimed at ensuring compliance with these clauses. In particular, the data importer undertakes to respond to investigations, to submit to audits and to comply with measures taken by the supervisory authority, including corrective and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary measures have been taken.

SECTION III: LOCAL LAW AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14. **Local law and practice affecting the enforcement of the clauses**

a) The parties submit that they have no reason to believe that the law and practices of the third country of destination applicable to the processing of personal data by the data importer, in particular the requirements for the communication of personal data or the measures for authorisation of access by public authorities, prevent the data importer from fulfilling its obligations under this specification. This assertion is based on the premise that this specification is not precluded by law and practice that essentially respects fundamental rights and freedoms and does not go beyond what is necessary and proportionate in a democratic society for safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

b) The parties declare that, in providing the security referred to in point (a), they have taken due account, in particular, of the following aspects:

I. the specific circumstances of the transfer, such as the length of the processing chain, the number of actors involved and the transmission channels used; the intended onward transfers; the type of recipient; the purpose of the processing; the categories and format of the personal data transferred; the economic sector in which the transfer takes place; the place of storage of the data transferred;
II. the law and practices of the third country of destination, in particular those requiring communication of data to public authorities or authorisation of access by such authorities, which are relevant to the specific circumstances of the transfer, as well as the applicable limitations and safeguards (12);
III. the relevant contractual, technical or organisational guarantees provided to supplement the guarantees provided for in this specification, in particular including the measures implemented during the transfer and processing of personal data in the country of destination.

c) The data importer ensures that, in carrying out the assessment referred to in point (b), it has made every effort to provide the data exporter with the relevant information and undertakes to continue to cooperate with the data exporter to ensure compliance with this specification.

d) The parties agree to document the assessment referred to in point (b) and to make it available to the competent supervisory authority upon request.

e) The data importer undertakes to promptly notify the data exporter if, after having become bound by this specification and during the term of the contract, it has reason to believe that it is or has been subject to regulations or practices which do not comply with the requirements of point (a), including following a change in the regulations in the third country or a measure (such as a request for communication) indicating an application of those regulations in practice which does not comply with the requirements of point (a).

f) If the notification referred to in point (e) is made or if the data exporter has reason to believe that the data importer is no longer able to fulfil its obligations under this Specification, the data exporter shall be obliged to notify the data importer in accordance with the provisions of this Specification.

(c) If the data exporter is not satisfied with the adequacy of the safeguards, the data exporter shall promptly determine the appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be taken by the data exporter and/or the data importer to remedy the situation [Module three: where applicable, after consultation with the controller]. The data exporter shall suspend the transfer of the data if it considers that there are no adequate safeguards or if so ordered by [Module three: the controller or] the competent supervisory authority. In this case, the data exporter shall be entitled to terminate the contract with regard to the processing of personal data under this specification. If the contract has more than two contracting parties, the data exporter may only exercise this right of termination in respect of the relevant party, unless the parties have agreed otherwise. In the event of termination of the contract under this clause, clause 16(d) and (e) shall apply.

Clause 15. **Obligations of the data importer in case of access by public authorities**

15.1. Notification

a) The data importer undertakes to promptly notify the data exporter and, where possible, the data subject (if necessary, with the assistance of the data exporter) if:

   I. receives a legally binding request for communication of personal data transferred in accordance with this specification from a public authority (in particular a judicial authority) under the law of the country of destination; such notification shall contain information on the personal data requested, the requesting authority, the legal basis for the request and the response given; or
   II. is aware that the public authorities have had direct access to the personal data transferred in accordance with this specification under the law of the country of destination; such notification shall include all information available to the data importer.

b) If the data importer is prohibited under the law of the country of destination from notifying the data exporter and/or the data subject, the data importer undertakes to make every effort to obtain a waiver of the prohibition in order to communicate all available information as soon as possible. The data importer undertakes to document its actions to this end in order to be able to justify its diligence if requested to do so by the data exporter.

c) To the extent permitted by the law of the country of destination, the data importer undertakes to provide the data exporter, at regular intervals during the term of the contract, with as much relevant information as possible on the requests received (in particular, the number of requests, the type of data requested, the requesting authority or authorities, the contestation of the requests, the outcome of such contestations, etc.).

d) The data importer undertakes to retain the information referred to in points (a) to (c) for the duration of the contract and to make it available to the competent supervisory authority upon request.

e) Points (a) to (c) are without prejudice to the obligation of the data importer, as referred to in Clause 14(e) and Clause 16, to promptly inform the data exporter when it is unable to comply with this specification.

15.2. Legality checks and data minimisation

a) The data importer undertakes to monitor the lawfulness of the request for communication and, in particular, whether the requesting public authority is duly empowered to do so, 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 law of the country of d e s t i n a t i o n , including obligations

applicable under international law and the principles of international comity. The data importer shall, under the same conditions, exhaust all other means of redress. When contesting a request, the data importer shall seek interim measures to suspend the effects of the request until the competent judicial authority has ruled on the merits. He shall not communicate the personal data requested until he is required to do so by the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b) The data importer undertakes to document its legal assessments and challenges to requests for disclosure and to make such documentation available to the data exporter to the extent permitted by the law of the country of destination. It shall also make such documentation available to the competent supervisory authority upon request. [Module three: The data exporter shall make the assessment available to the controller.

c) The data importer undertakes to provide as little information as possible when responding to requests for communication, based on a reasonable interpretation of the request.

SECTION IV: FINAL PROVISIONS

Clause 16. **Non-performance of clauses and termination of the contract**

a) The data importer shall promptly inform the data exporter if it is unable to comply with this specification for any reason.

b) In the event that the data importer is in breach of its obligations under this specification, the data exporter shall suspend the transfer of personal data to the data importer until such time as performance is assured again or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract in respect of the processing of personal data under this specification where:

   I. the data exporter has suspended the transfer of personal data to the data importer in accordance with point (b) and compliance with this specification is not resumed within a reasonable period of time and in any event within one month of the suspension;
   II. the data importer is in substantial or persistent breach of these specifications; or
   III. the data importer fails to comply with a binding decision of a competent court or supervisory authority in relation to its obligations under this specification.

   In this case, it shall inform the competent supervisory authority [module three: and the controller] of its breach. If the contract has more than two contracting parties, the data exporter may only exercise this right of termination with respect to the relevant party, unless the parties have agreed otherwise.

d) Personal data which have been transferred before termination of the contract pursuant to point (c) shall, at the option of the data exporter, be returned immediately to the data exporter or destroyed in their entirety. The same shall apply to copies of the data]. [Module four: Personal data collected by the data exporter in the EU which have been transferred prior to the termination of the contract pursuant to point (c) shall be destroyed in their entirety immediately, as well as any copies thereof]. The data importer shall provide evidence of the destruction of the data to the data exporter. Until the data are destroyed or returned, the data importer shall continue to ensure compliance with this Specification. If the law of the country applicable to the data importer prohibits the return or destruction of the transferred personal data, the data importer undertakes to continue to

ensuring compliance with this specification and shall process the data only to the extent and for the duration required by national law.

e) Neither party may withdraw its consent to be bound by this Specification if: (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 regulating the transfer of personal data to which this Specification applies; or (ii) Regulation (EU) 2016/679 becomes part of the law of the country to which the personal data are transferred. This is without prejudice to other responsibilities that apply to the processing in question under Regulation (EU) 2016/679.

Clause 17. **Applicable law**

These clauses shall be governed by the law of one of the EU Member States, provided that such law permits the rights of third party beneficiaries. The Parties agree that this shall be the law of Spain.

Clause 18. **Choice of forum and jurisdiction**

a) Any dispute arising from these specifications shall be judicially settled in a Member State of the European Union.
b) The parties agree that the courts of Spain shall have jurisdiction.
c) Data subjects may also bring legal proceedings against the data exporter and/or the data importer in the Member State in which the data subject has his or her habitual residence.
d) The parties agree to submit to the jurisdiction of that Member State.

Clause 19. **Additional Safeguards**

The data importer undertakes to implement the additional safeguards specified in **Section 3: Security measures.**

APPENDIX

ANNEX I

A. LIST OF PARTS

Data exporter(s):

Name: **CTAIMA OUTSOURCING Y CONSULTING S.L. -** B43715812
Address: Salvador Espriu, 18, Tarragona 43007, Spain
Name, position and contact details: Lorenzo de Zavala, Legal Representative, administracion@ctaima.com

Activities related to the data transferred under these clauses:
The data importer provides the Services to the data exporter in accordance with an agreement between the parties.

The services consist of the provision of review, validation and uploading of documentation to business coordination platforms.

Lorenzo de Zavala
4/12/2023
Function: Data Controller.

Data importer(s):

Name: **CTAIMA COLOMBIA S.A.S.** - 901717143-1
Address: Cra. 12 No. 89-33, Bogotá D.C. 110211, Colombia
Name, position and contact details: Luis de los Santos, Legal Representative, administracion@ctaima.com

Activities related to the data transferred under these clauses:

The data importer provides the review, validation and uploading services to business coordination platforms applicable to the data exporter in accordance with the Agreement between the parties.

Luis de los Santos
4/12/2023
Function: Processor.

B. DESCRIPTION OF THE TRANSFER

Categories of data subjects whose personal data are transferred

- Client/contractor workers.

Categories of personal data transferred

- Identification data (name and surname), position, e-mail and telephone number of the users of t h e client's application.
- Identification data (name and surname), position, e-mail and telephone number of the client's contractors.
- Identification data (name and surname), position, e-mail and telephone number of our clients' customers.

- Identification data (name and surname), employment data and occupational risk prevention data (business coordination) of the contractor's workers.

Treatment activities.
Frequency of transfer: Continuous.

Nature of treatment

The nature of the processing is to provide the Services to the Controller in accordance with the Contract, and in accordance with any further instructions given by the Controller.

Purpose of data transfer and further processing

Provision of review, validation and uploading of documentation to business coordination platforms. There is no post-processing after the end of the agreement.

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

The data importer shall retain the Transferred Personal Data until their deletion in accordance with the data exporter's guidelines for their destruction or return.

No subcontracting takes place.

C. COMPETENT SUPERVISORY AUTHORITY

Spanish Data Protection Agency. C/ Jorge Juan, 6. 28001 - Madrid. Tel. 900 293 183. www.aepd.es

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES, INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE DATA SECURITY

1. Information security policies: Implement information security policies that establish standards and procedures to protect personal data transferred. The company establishes policies and procedures to protect the transfer of information in order to prevent its unauthorised interception, copying, modification or destruction.
2. Work on the review and validation of documents exclusively remotely with the IT systems of the data controller, and it is expressly forbidden to download documents containing personal data onto the data processor's own IT systems in the country where the data processor is located.
3. Data encryption: encrypt all sensitive information during transfer and storage to prevent unauthorised access.
4. Access control: implement access control systems that limit access to data to authorised personnel only, by assigning roles and permissions. Facilities shall be protected by physical entry control to ensure access only to authorised personnel. All visits will be supervised and controlled.
5. Access monitoring and logging: Establish an access monitoring and logging system to record and supervise all activities related to transferred data. The company monitors its information and processing systems hosted in the cloud using the Microsoft Azure Monitor service to detect unauthorised activities and logs them as security incidents, reviewing the operation and failure log of its systems to identify the problem.
6. The company manages and controls its network to protect it from unauthorised access, maintain the security of its systems and applications that use it, including information in transit.
7. Security updates and patches: keep all systems and applications up to date with the latest security patches to mitigate vulnerabilities. Vulnerabilities identified in critical environments will be logged and a person responsible for managing and coordinating vulnerability remediation will be assigned.
8. Malware protection: implement malware protection measures, such as firewalls, anti-virus and anti-malware, to prevent infections and cyber attacks. The company implements controls for detection, prevention and recovery that protect information systems along with appropriate staff awareness. The company establishes these policies in order to maintain the confidentiality, availability and integrity of information on its systems.
9. Data backup and recovery: establish regular backup procedures for transferred data and recovery systems in case of failures or security incidents.
10. Staff training and awareness: provide regular information security training and awareness to staff to ensure compliance with established policies and procedures.
11. Security audits: conduct regular security audits to assess the effectiveness of implemented measures and to detect possible vulnerabilities.
12. Security incident management: establish a security incident management plan that includes timely notification of any security breaches to the Data Protection Officer and competent authorities.
13. Risk assessment: conduct regular information security risk assessments to identify and mitigate potential threats and vulnerabilities.

These technical and organisational measures will help to ensure the security of data transferred outside the European Union, thereby complying with the data protection requirements set out in the Standard Contractual Clauses Contract.

ANNEX III - LIST OF SUB-PROCESSORS

No subcontracting takes place.

CTAIMA COLOMBIA S.A.S.

Name: Luis de los Santos
Position: Legal Representative

CTAIMA OUTSOURCING AND CONSULTING S.L.

Name: Lorenzo de Zavala
Position: Legal Representative