

STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS

SECTION I

Clause 1. Purpose and scope of application

- 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 agency(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 data exporter's personal data directly or indirectly through another entity that is also a party to these terms and conditions, listed in Annex I.A (each hereinafter referred to as a "data importer"), have agreed to these standard contractual terms and conditions (hereinafter referred to as "terms and conditions").
- c) These specifications apply to the transfer of personal data specified in Annex I.B.
- d) The appendix to the present bidding documents, which contains the annexes cited therein, are part of the bidding documents.

Clause 2. Effect and invariability of clauses.

- a) This specification provides 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 appendix information. This does not preclude the parties from including in a broader contract the standard contractual clauses contained in this specification, 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 the 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 invoke, as third party beneficiaries, these specifications against the exporter and/or the data importer and require them to comply with them, 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, letters a), c), d) and e); [module three] clause 9, letters 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, letters c), d) and e).
- VII. Clause 16, letter e).
- VIII. Clause 18: [modules one, two and three] clause 18 (a) and (b); [module four] clause 18.

- b) The provisions of point a) are without prejudice to the rights granted to data subjects by Regulation (EU) 2016/679.

Clause 4. **Interpretation**

- a) Where terms defined in Regulation (EU) 2016/679 are used in these specifications, they are understood to have the same meaning as in that Regulation.
- b) These specifications shall be read and interpreted in accordance with the provisions of Regulation (EU) 2016/679.
- c) This specification 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 the present bidding documents and the provisions of related agreements between the parties in effect at the time these bidding documents were agreed upon or commenced to be applied, these bidding documents shall prevail.

Clause 6. **Description of the transfer or transfers**

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

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

- a) Any entity that is not a party to these terms and conditions may, subject to the consent of all parties, accede to these terms and conditions 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 terms and conditions 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 organizational measures, meet its obligations under these terms and conditions.

8.1. Instructions

- a) The data importer shall only process personal data in accordance with documented instructions from the data exporter. The data exporter may give such instructions during the entire term 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 the personal data only for the specific purposes of the transfer indicated in Annex I.B, except when following additional 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 these terms and conditions, including the appendix completed by the parties. To the extent necessary to protect trade 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 appendix to these terms and conditions before sharing a copy, but shall provide a meaningful summary if failure to do so would prevent the data subject from understanding the contents of the appendix or exercising his or her rights. Upon request, the parties shall communicate the reasons for the redaction to the party concerned, to the extent possible without disclosing the redacted information. This clause is without prejudice to the obligations placed on the data exporter by 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 outdated, 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

Processing by the Data Importer shall only be carried out for the period specified in Annex I.B. Once the processing services have been provided, the Data Importer shall, at the Data Exporter's request, 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 is destroyed or returned, the data importer shall continue to ensure compliance with these terms and conditions. If the law of the country applicable to the data importer prohibits the return or destruction of the personal data, the data importer undertakes to continue to ensure compliance with these terms and conditions 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 data importer's obligation under this clause to inform the data exporter throughout the term 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. Treatment safety

- a) The data importer and, during the transfer, also the data exporter shall implement appropriate technical and organizational 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 unauthorized disclosure or access (hereinafter referred to as "personal data security 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 consider, in particular, encryption or pseudonymization, especially during transmission, if the purpose of the processing can be fulfilled in this way. In the case of pseudonymization, the additional information necessary to attribute the personal data to a specific data subject shall, 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 organizational measures set out in Annex II. The

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

- b) The data importer shall only grant access to personal data to members of its staff to the extent strictly necessary for the performance, management and monitoring of the contract. It shall ensure that the persons authorized 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. When and to the extent that all information cannot be provided at the same time, the initial notification shall provide the information currently available and, as it becomes available, additional information shall be provided without undue delay.
- d) The data importer shall cooperate with and assist the data exporter to enable it to comply with its obligations under Regulation (EU) 2016/679, especially as regards notification to the competent supervisory authority and 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 concerning criminal convictions and offences (hereinafter referred to as "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Subsequent transfers

The data importer shall only disclose personal data to a third party upon documented instructions from the data exporter. Furthermore, 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 these terms and conditions, with the choice of the relevant module, or if:

- I. the onward transfer is directed to a country for which an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 covering the onward transfer has been issued;
- II. the third party otherwise provides adequate safeguards pursuant to Article 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- III. if the onward transfer is necessary for the formulation, exercise or defense 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 another natural person. The validity of onward transfers depends on the data importer providing the other assurances provided for in these terms and conditions, in particular the purpose limitation.

8.9. Documentation and compliance

- a) The data importer shall promptly and appropriately resolve the data exporter's queries related to the processing in accordance with these terms and conditions.
- b) The parties must be able to demonstrate compliance with these terms and conditions. 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 under this specification and, at the 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 authorize an independent auditor. Audits may consist of inspections of the data importer's physical premises or facilities and, where appropriate, be conducted with reasonable notice.
- e) The parties shall make available to the competent supervisory authority, at its request, the information referred to in points b) and c) and, in particular, the results of the audits.

Clause 9. Use of Subcontractors

- 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 authorization of the Data Exporter. The data importer shall submit the request for specific authorization 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 authorization. The list of sub-agents already authorized by the data exporter is contained in Annex III. The Parties shall keep Annex III updated.
- 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 subcontractor complies with the obligations attributed to it by these specifications.
- c) The data importer shall provide the data exporter, at the data exporter's request, with a copy of the contract with the subcontractor 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 such 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 the data exporter has authorized it to do so.
- b) The data importer shall assist the data exporter in fulfilling its obligations when responding to requests for the exercise of rights attributed to data subjects by Regulation (EU) 2016/679. In this regard, the parties shall set out in Annex II appropriate technical and organizational 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 the obligations under letters a) and b), the data importer shall follow the instructions of the data exporter.

Clause 11. Remedies

- 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 authorized point of contact 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 recourse mechanism and that they are not obliged to use it or to follow a particular sequence in seeking recourse.

- b) In the event of a dispute between an interested party and one of the Parties regarding the performance of the present clauses, such Party shall make every effort to resolve the matter amicably in a timely manner. The Parties shall keep each other informed of such disputes and, where appropriate, shall cooperate to resolve them.
- c) Where the data subject invokes a third-party beneficiary right under Clause 3, the data importer shall accept the data subject's decision to
 - I. submit a complaint to the supervisory authority of the Member State of his habitual residence or place of work, or to 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, organization 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 the data subject's substantive and procedural rights to seek remedies under 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 receive compensation, for any material or non-material damages that the data importer or its sub-agent causes 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 caused to the data subject by the data exporter or the data importer (or its sub-processor) as a result of the violation of 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, to 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 subsection (c) for damage caused by the data importer (or its subcontractor), 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 be entitled to bring an action against any of these Parties.
- f) The Parties agree that, if one of them 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 subcontractor to avoid its own liability.

Clause 13. **Supervision**

- a) Where the data exporter is established in an EU Member State:] The supervisory authority responsible for ensuring the data exporter's compliance with Regulation (EU) 2016/679 with regard to the transfer of data, as indicated 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 designate 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 are transferred pursuant to these Clauses in connection with the offering of goods or services to them, or whose behavior is monitored, as referred to in Annex I.C, shall act as the competent supervisory authority.

- 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 compliance with the clauses.

- a) The parties state 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 authorizing access by public authorities, prevent the data importer from fulfilling its obligations under this specification. This assertion is based on the premise that the law and practices that essentially respect fundamental rights and freedoms and do not go beyond what is necessary and proportionate in a democratic society for the purpose of safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- b) The parties declare that, in providing the guarantee referred to in letter a), they have duly taken into account, in particular, 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 transferred data;
 - II. the law and practices of the third country of destination - especially those requiring communication of data to public authorities or authorizing access by such authorities - that are relevant to the specific circumstances of the transfer, as well as the applicable limitations and safeguards (12);
 - III. the relevant contractual, technical or organizational guarantees provided to supplement the guarantees provided for in these specifications, in particular including the measures implemented during the transfer and processing of personal data in the country of destination.
- c) The data importer assures that, in carrying out the assessment referred to in b) above, 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 these terms and conditions.
- d) The parties agree to document the assessment referred to in letter b) and make it available to the competent supervisory authority upon request.
- e) The data importer undertakes to promptly notify the data exporter if, after becoming bound by these terms and conditions and during the term of the contract, it has reason to believe that it is or has been subject to regulations or practices that do not conform to the requirements of letter 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 such regulations in practice that does not conform to the requirements of letter 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 can no longer meet its obligations under these terms and conditions, the data importer shall be required to notify the data exporter in writing.

If the data exporter considers that there are no adequate safeguards (e.g., technical or organizational measures to ensure security and confidentiality) to be taken by the data exporter and/or data importer to remedy the situation [module three; if applicable, after consultation with the controller], the data exporter shall promptly determine the appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be taken by the data exporter and/or data importer to remedy the situation [module three; if 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 respect 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 with respect to the relevant party, unless the parties have agreed otherwise. In the event of termination of the contract pursuant to 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 pursuant to 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 pursuant to 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 from sending the notification to the data exporter and/or the data subject under the law of the country of destination, 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 the actions it takes 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 keep the information referred to in letters 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) shall be without prejudice to the obligation of the data importer, referred to in clause 14, letter e), and in clause 16, to promptly inform the data exporter when it is unable to comply with these terms and conditions.

15.2. Legality control and data minimization

- a) The data importer undertakes to monitor the legality 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 destination, including obligations

applicable under international law and the principles of international comity. The data importer shall, under the same conditions, exhaust the remedies available. When contesting a request, the data importer shall request the application of interim measures to suspend the effects of the request until the competent judicial authority has ruled on the merits. It shall not communicate the personal data requested until it is required to do so by the applicable procedural rules. These requirements are without prejudice to the obligations attributed to the data importer by clause 14, letter e).

- b) The data importer undertakes to document its legal assessments and challenges to communication requests 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 data 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 these terms and conditions for any reason whatsoever.
- b) In the event that the data importer fails to comply with its obligations under these terms and conditions, 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. The foregoing is without prejudice to clause 14, letter f).
- c) The data exporter shall be entitled to terminate the contract with respect to the processing of personal data under these terms and conditions when:
 - I. the data exporter has suspended the transfer of personal data to the data importer in accordance with letter b) and the data exporter does not comply with these terms and conditions within a reasonable period of time and, in any case, 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 these specifications.

In this case, it shall inform the competent supervisory authority [module three: and the data 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 that have been transferred prior to the termination of the contract pursuant to (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 that have been transferred prior to the termination of the contract pursuant to (c) shall be destroyed in their entirety immediately, as well as any copies thereof]. The data importer shall credit the destruction of the data to the data exporter. Until the data is destroyed or returned, the data importer shall continue to ensure compliance with these terms and conditions. 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 these terms and conditions and will only process the data to the extent and for the time required by the law of the country.

- 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 governing the transfer of personal data to which this specification applies; or (ii) Regulation (EU) 2016/679 becomes part of the legal system of the country to which the personal data is 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 allows 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 take legal action against the data exporter and/or 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 apply the additional safeguards specified in **Section 3: Security measures**.

APPENDIX

ANNEX I

A. PARTS LIST

Data exporter(s):

Name: **CTAIMA OUTSOURCING Y CONSULTING S.L.** - B43715812

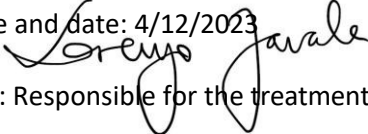
Address: Salvador Espriu, 18, Tarragona 43007, Spain

Name, position and contact information: 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 reviewing, validating and uploading documentation to business coordination platforms.

Signature and date: 4/12/2023


Function: Responsible for the treatment.

Data importer(s):

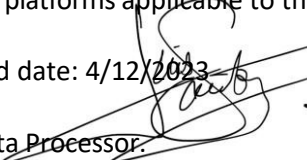
Name: **CTAIMA COLOMBIA S.A.S.** - 901717143-1

Address: Cra. 12 No. 89-33, Bogotá D.C. 110211, Colombia

Name, position and contact information: Luis de los Santos, Legal Representative, administracion@ctaima.com

Activities related to the data transferred under these clauses:

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

Signature and date: 4/12/2023


Function: Data Processor.

B. DESCRIPTION OF THE TRANSFER

Categories of data subjects whose personal data is transferred

- Client/contractor workers.

Categories of personal data transferred

- Identification data (name and surname), position, e-mail and telephone number of the client's application users.
- 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), labor and occupational risk prevention (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 additional 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 its deletion in accordance with the guidelines of the data exporter consisting of its destruction or return.

There is no subcontracting.

C. COMPETENT SUPERVISORY AUTHORITY

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


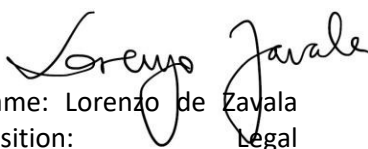
ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE DATA SECURITY

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 interception, copying, modification or unauthorized destruction.
2. Work the revision and validation of documents exclusively remotely with the IT systems of the person in charge, being expressly forbidden to download documents containing personal data in the IT systems of the person in charge in his country of location.
3. Data encryption: encrypt all sensitive information during transfer and storage to prevent unauthorized access.
4. Access control: Implement access control systems that limit access to data to authorized personnel only, by assigning roles and permissions. The facilities will be protected by a physical entry control that guarantees access only to authorized 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 performs monitoring of its information and processing systems hosted in the cloud using the Microsoft Azure Monitor service to detect unauthorized activities and recording 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 unauthorized 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 updated 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, antivirus 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 the information in its systems.
9. Data backup and recovery: establish regular backup procedures for transferred data and recovery systems in the event 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: perform periodic security audits to evaluate the effectiveness of the measures implemented and detect possible vulnerabilities.
12. Security incident management: establish a security incident management plan that includes timely notification of any security breach to the Data Protection Officer and the competent authorities.
13. Risk assessment: conduct periodic information security risk assessments to identify and mitigate potential threats and vulnerabilities.

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

ANNEX III - LIST OF SUB PROCESSORS

There is no subcontracting.

CTAIMA COLOMBIA S.A.S.	CTAIMA OUTSOURCING AND CONSULTING S.L.
 <p>Name: Luis de los Santos Position: Legal Representative DNI: 51112090H</p>	 <p>Name: Lorenzo de Zavala Position: Legal Representative DNI: 50906094X</p>