AWARE DATA PROCESSING AGREEMENT

Last Modified: May 30, 2024

This Data Processing Agreement (this "Agreement" or this "DPA") is made and entered by and between:

Aware, Inc., a company organized and existing under the laws of the Commonwealth of Massachusetts, with a registered address located at 76 Blanchard Road, Burlington, Massachusetts 01803 U.S.A. (hereinafter "Aware" or "Data Processor"), and

The Aware Business Customer (hereinafter the "Customer" or "Data Controller") that has entered into a Contract for Services or Software ("Principal Agreement").

Aware and the Customer may be referred to herein as "Party" individually or "Parties" collectively.

This DPA forms a part of the Contract for Services or Software ("Principal Agreement") between the Parties. By executing the Principal Agreement, Customer unequivocally agrees to be bound by and a party to this DPA which forms an integral part of the Principal Agreement.

1. Definitions

"Argentinian Personal Information" means Personal Data that is subject to the protection of the Argentine Law No. 25.326, Regulatory Decree No. 1558/07 and subsequent decrees.

"Brazilian Personal Information" means Personal Data that is subject to the protection of the Brazilian Data Protection Law ("LGPD") (Law No. 13,853/2019).

"California Personal Information" means Personal Data that is subject to the protection of the CPRA.

"CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2020), as amended by the California Privacy Rights Act ("CPRA"), and inclusive of implementing regulations.

"Consumer", "Business", "Sell" and "Service Provider" will have the meanings given to them in the CPRA.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws" means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.

"Data Subject" means the individual to whom Personal Data relates.

"Data Privacy Framework" means the EU-US Data Privacy Framework (EU-US DPF), the UK Extension to the EU-US Data Privacy Framework (UK Extension to the EU-US DPF), and the Swiss-US Data Privacy Framework (Swiss-US DPF) program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to its Decision of July 10, 2023, by UK Extension to the EU-US DPF effective October 12, 2023, and Swiss-US DPF when an adequacy decision is reached.

"Europe" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

“European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

"European Data Protection Laws" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

"Permitted Affiliates" means any of your Affiliates that (i) are permitted to use the Subscription Services pursuant to the Agreement, but have not signed their own separate agreement with us and are not a “Customer” as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws.

“Personal Data” means any information relating to an identified or identifiable individual where (i) such information is contained within Customer Data; and (ii) is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process,” “Processes,” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021 currently found at https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf, as may be amended, superseded or replaced.

“Sub-Processor” means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Subscription Services under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any Aware employee or consultant.

“UK Addendum” means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 currently found at https://ico.org.uk/media/fororganisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended, superseded, or replaced.

“UK Data” means Personal Data that is subject to the protection of the UK GDPR and Data Protection Act 2018.

2. Customer Responsibilities

a. Compliance with Laws. Within the scope of the Agreement and in its use of the services, you will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to us.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data (as that term is defined within the Principal Agreement) and the means by which you acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes); (iii) ensuring you have the right to process and transfer, or otherwise provide access to, the Personal Data to us for Processing in accordance with the terms of the Principal Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Subscription Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. You will inform us without undue delay if you are not able to comply with your responsibilities under this 'Compliance with Laws' section or applicable Data Protection Laws.

b. Controller Instructions. The parties agree that the Principal Agreement (including this DPA), together with your use of the Services or Software in accordance with the Principal Agreement, constitute your complete instructions to us in relation to the Processing of Personal Data, so long as you may provide additional instructions during the subscription term that are consistent with the Principal Agreement, the nature and lawful use of the Services or Software.

c. Security. You are responsible for independently determining whether the data security provided for in the Services or Software adequately meets your obligations under applicable Data Protection Laws. You are also responsible for your secure use of the Services or Software, including protecting the security of Personal Data in transit to and from the Services or Software (including to securely backup or encrypt any such personal data).

3. Aware Obligations

a. Compliance with Instructions. We will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

b. Conflict of Laws. If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we can comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Services until such time as you issue new lawful Instructions with regard to the Processing.

c. Security. We will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

d. Confidentiality. We will ensure that any personnel whom we authorize to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. Personal Data Breaches. We will notify you without undue delay after we become aware of any Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as is necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws. We will co-operate with you and take any reasonable steps that you direct us to take in order to assist with the investigation, mitigation, and remediation of any such Personal Data Breach.

f. Deletion or Return of Personal Data. We will delete all Customer Data, including Personal Data (including copies thereof) Processed pursuant to this DPA, on the termination or expiration of your Services or Software in accordance with the procedures set out in the Principal Agreement. This term will apply except where we are required by applicable law to retain some or all of the Customer Data, or where we have archived Customer Data on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with our deletion practices. You may request the deletion of the Customer Data after the expiration or termination of the Principal Agreement by emailing us at privacy@aware.com.

4. Data Subject Requests

The Service or Software provides you with a number of controls that you can use to retrieve, correct, delete or restrict Personal Data, which you can use to assist it in connection with its obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

To the extent that you are unable to independently address a Data Subject Request through the Service or Software, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Principal Agreement. You will reimburse us for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Principal Agreement is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

5. Sub-Processors

You agree that we may engage Sub-Processors to Process Personal Data on your behalf. We have currently appointed, as Sub-Processors, the third parties listed in Annex 3 to this DPA.

Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.

6. Data Transfers

Other than as specified under Section 7, below, you acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Services in accordance with the Principal Agreement, and in particular that Personal Data may be transferred to and Processed by Aware in the United States and to other jurisdictions where our Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

7. Additional Provisions for Processing European Data under the EU or UK GDPR

a. Scope. This Section 7 will apply only with respect to European Data.

b. Roles of the Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of European Data and we are the Processor.

c. Instructions. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.

d. Objection to New Sub-Processors. We will give you the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 30 days of notifying you in accordance with the "Sub-Processors" section. If you do not notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Service and/or Software in accordance with the terminations of the Principal Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination).

e. Sub-Processor Agreements. You acknowledge that we may be restricted from disclosing Sub-Processor agreements but we will use reasonable efforts to require any Sub-Processor we appoint to permit it to disclose the Sub-Processor agreement to you and will provide (on a confidential basis) all information we reasonably can.

f. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities (for example, the French Data Protection Agency (CNIL), the Berlin Data Protection Authority (BlnBDI) and the UK Information Commissioner's Office (ICO)) or other competent data privacy authorities to the extent required by European Data Protection Laws.

g. Data Transfers from Europe to the U.S.. Transfers of Personal Data from Europe to the U.S. will occur pursuant to the Data Protection Framework, under which Aware is certified.

h. Demonstration of Compliance. We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA. You acknowledge and agree

8. Additional Provisions for California Personal Information

a. Scope. This Section 8 will apply only with respect to California Personal Information.

b. Roles of the Parties. When Processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that, where applicable, you are the Business and we are the Service Provider.

c. Obligations as Service Provider: We will only process California Personal Information for a business purpose on behalf of you, and will not process California Personal Data for any other purpose unless permitted by the CPRA.

d. Limitations on Processing: We will not (a) take any action that would meet the definition of "selling personal information" or "sharing personal information" under the CCPA; (b) retain, use, or disclose California Personal

Information for any purpose other than for a business purpose pursuant to the Services Agreement; (c) combine California Personal Information with any other data if this would be inconsistent with the limitations on service providers under the CCPA.

9. Additional Provisions for Brazilian Data

a. Scope. This Section 9 will apply only with respect to Brazilian Data.

b. Roles of the Parties. When Processing Brazilian Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of Brazilian Data and we are the Processor.

c. Instructions. If we believe that your Instruction infringes the Brazilian Data Protection Law (where applicable), we will inform you without delay.

d. Security Incidents Involving Personal Data. We will notify you without undue delay after we become aware of any security incident that may create risk or relevant damage to the data subjects as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as is necessary to enable you to notify relevant security incidents to competent authorities and affected Data Subjects, if you are required to do so under Brazilian Data Protection Law. We will co-operate with you and take any reasonable commercial steps that you direct us to take in order to assist with the investigation, mitigation, and remediation of any such security incident that may create risk or relevant damage to the data subjects.

e. Transfer Mechanisms for Data Transfers. The country where we will process Personal Data is set forth in Annex 1. Where required by Brazilian Data Protection Law, the Parties will enter into standard contractual clauses to ensure an adequate level of data protection for the international transfer of controller's Personal Data to processor. The Parties will enter into standard contractual clauses, as set forth in Annex 4. The Parties agree and stipulate that EU GDPR standard contractual clauses provide an adequate level of data protection under Brazilian Data Protection Law and will use these standard contractual clauses unless and until Brazilian law provides its own standard contractual clauses and the Parties determine that these standard contractual clauses materially differ. The Parties will be bound by these standard contractual clauses unless and until Brazilian regulatory authorities determine that the country of our processing provides an adequate level of data protection in accordance with Brazilian Data Protection Law.

10. Additional Provisions for Argentinian Personal Data

a. Scope. This Section 10 will apply only with respect to Argentinian Personal Data.

b. Roles of the Parties. When Processing Argentinian Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of Argentinian Data and we are the Processor.

c. Instructions. If we believe that your Instruction infringes the Argentinian Data Protection Law (where applicable), we will inform you without delay.

d. Security Incidents Involving Personal Data. We will notify you within seventy-two hours of becoming aware of a Personal Data breach. At your request, we will promptly provide you with such reasonable assistance as is necessary to enable you to notify relevant security incidents to competent authorities and affected Data Subjects, if you are required to do so under Argentinian Data Protection Law. We will co-operate with you and take any reasonable commercial steps that you direct us to take in order to assist with the investigation, mitigation, and remediation of any such security incident that may create risk or relevant damage to the data subjects.

f. Transfer Mechanisms for Data Transfers. The country where we will process Personal Data is set forth in Annex 1. The Parties will enter into Model Contractual Clauses, as set for in Annex 4, to ensure an adequate level of data protection for the international transfer of Controller's Personal Data to Processor. Module Two will apply to the extent that you are a Controller and we are a Processer of Personal Data. Annexes A and B of the Model Contractual Clauses shall be deemed completed with the information set out in Annex 1 to this Agreement; Annex C of the Model Contractual Clauses shall be deemed completed with the information set out in Annex 2 to this Agreement; Annex D of the Model Contractual Clauses shall be deemed completed with the information set out in Annex 3 to this Agreement.

11. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Principal Agreement and without prejudice to the "Compliance with Instructions" or "Security" sections of this DPA, we reserve the right to make any updates and changes to the DPA with or without notice to you.

b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

c. Limitation of Liability. The Parties agree that the limitations and exclusions of liability set out in the Principal Agreement shall apply in respect of a Party's liability arising out of, or in connection with, this DPA. The Parties agree that no limitations or exclusions of liability set out in the Principal Agreement shall apply to any Party's liability to data subjects to the extent that such limitations or exclusions are prohibited by applicable data protection laws.

d. Governing Law. The Parties agree that, with the exception of substantive provisions under applicable Data Protection Laws, this DPA will be governed by the laws of the Commonwealth of Massachusetts unless otherwise provided for in the Principal Agreement. In the event of a dispute between this clause and the Principal Agreement, the Principal Agreement shall control.

e. Jurisdiction. Any dispute arising in connection with this DPA will be submitted to the exclusive jurisdiction of the state or federal courts in Massachusetts, and the parties irrevocably consent to the exclusive jurisdiction of such courts. In the event of a dispute between this clause and the Principal Agreement, the Principal Agreement shall control.

12. Parties to this DPA

a. Permitted Affiliates. By signing the Agreement, you enter into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of yourself and in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms "Customer", "you" and "your" will include you and such Permitted Affiliates.

b. Authorization. The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. Remedies. The parties agree that (i) solely the Customer entity that is the contracting party to the Principal Agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all Instructions, authorization and communications with us under the DPA and will be entitled to make and receive any communications related to this DPA on behalf of its Permitted Affiliates.

d. Other rights. The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance" section, take all reasonable measures to limit any impact on us and our Affiliates by

combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Principal Agreement and all of its Permitted Affiliates in one single audit.

Annex 1 – Details of Processing

A. List of Parties

Data Exporter:

Name: The Customer, as defined in the DPA (on behalf of itself and Permitted Affiliates)

Address: The Customer's address, as set out in the Principal Agreement

Contact Person's Name, Position and Contact Details: The Customer's contact details, as set out in the Principal Agreement

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Aware Services and/or Software under the Principal Agreement

Role (controller/processor): Controller

Data Importer:

Name: Aware, Inc.

Address: 76 Blanchard Road, Burlington, MA 01803, USA

Contact Person's Name, Position and Contact Details: Avena Moran, Data Protection Officer, privacy@aware.com

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with the Customer's use of the Aware Services and/or Software under the Principal Agreement

B. Description of Transfer

Categories of Data Subjects whose Personal Data is Transferred

You may submit Personal Data in the course of using the Services and/or Software, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to the Personal Data relating to the following categories of Data Subjects:

Your contacts and other end users including your employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.

Categories of Personal Data Transferred

You may submit Personal Data to the Services and/or Software, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

- Contact information (as defined in the General Terms)
- Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Services and/or Software

Sensitive Data transferred and applied restrictions or safeguards

You may submit Sensitive Data, including Biometric Identifiers, to the Services and/or Software, the extent to which is determined and controlled by you in your sole discretion. You must inform the individual from whom the Biometric Data will be collected, in writing and prior to collecting his or her Biometric Identifiers, that the Biometric Identifiers are being collected. You must also indicate, in writing, the specific purpose(s) and length of time for which the Biometric Identifiers are being collected,

stored and/or used and receive a written release from the individual authorizing you and your service providers, including Aware, to collect, store and/or use the Biometric Identifiers and authorizing you to disclose such Biometric Identifiers to Aware and Aware's sub-processors, where applicable.

Frequency of transfer

Continuous

Nature of the Processing

Personal Data will be Processed in accordance with the Principal Agreement (including this DPA) and may be subject to the following Processing activities:

- Storage and other Processing necessary to provide, maintain and improve the Services and/or Software provided to you; and/or
- Disclosure in accordance with the Principal Agreement (including this DPA) and/or as compelled by applicable laws.

Purpose of the transfer and further processing

We will Process Personal Data as necessary to provide the Services and/or Software pursuant to this DPA and the Principal Agreement, and as further instructed by you in your use of the Services and/or Software.

Period for which Personal Data will be retained

Subject to the "Deletion of Personal Data" section of the DPA, we will Process Personal Data for the duration of the Principal Agreement, unless otherwise agreed in writing, and retain Personal Data in accordance with Aware's Data Security & Privacy Policy, as may be amended from time to time, available at https://www.aware.com/dataprivacy/ .

C. Competent Supervisory Authority

For the purposes of the Standard Contractual Clauses, if applicable, the supervisory authority that will act as a competent supervisory authority will be determined in accordance with GDPR.

Annex 2 – Security Measures

We have implemented Information Security Program (including enforcement of internal policies and procedures) designed to help secure your data against accidental or unlawful loss, access, or disclosure, and unauthorized access to the Aware Network.

Additional security measures outlined below –

1. Protect data while at rest, in motion and in use within applications
2. Granular privilege management (permissions, etc.) is implemented to govern the access to, use of, and disposition of data.
3. Approved standards for security markings, handling restrictions, and records management.
4. Only authorized users are able to access and share data.
5. Access, use, and disposition of data are fully audited.
6. Classification and control markings are defined and implemented, content and record retention rules are developed and implemented.
7. Prevent unintended release and disclosure of data.
8. Security Incident – Notify customer of a Security Incident without undue delay after becoming aware of the Security Incident. Measures are in place to mitigate any adverse effects resulting from the Security Incident.
9. Physical Security – Physical controls are in place to prevent unauthorized entrance to the facilities.
10. Network Security – Access controls and policies are in place to manage access management. Controls are in place to maintain corrective action and incident response to respond to potential security threats.
11. Continued Evaluation – Aware conducts periodic reviews of the Aware Network and security posture measured against industry standards and its policies and procedures.

Annex 3 – List of Sub-Processors

Third-Party Sub-Processor	Purpose	Applicable Service	Data Center Sub-Processor Location
Amazon Web Services, Inc.	**Cloud Infrastrcture Provider**	**https://aws.amazon.com/**	**United States**
ID Dataweb*	**Identity Verification**	**https://www.iddataweb.com/**	**United States**
PDK*	**Access Control Service**	**https://pdk.io**	**United States**
Regula*	**Document Verification**	**https://regulaforensics.com/**	**United States**

***You may choose not to use the functionality provided by our Sub-Processors marked with an asterisk above, depending upon the Service(s) and/or Software you have subscribed to pursuant to the Principal Agreement.

Annex 4

RED IBEROAMERICANA DE PROTECCION DE DATOS

IBERO-AMERICAN DATA PROTECTION NETWORK

Annex

MODEL CONTRACTUAL CLAUSES

Content

NOTE: The use of these model contractual clauses requires prior reading the respective Explanatory Guide in order to identify their suggested use and the scope of the document. It is the sole responsibility of the person who processes Personal Data to demonstrate compliance with the respective regulatory requirements or to turn to the competent Supervisory Authority/ies to confirm their proper use.

1.

MODEL AGREEMENT FOR THE INTERNATIONAL TRANSFER OF PERSONAL DATA FROM *CONTROLLER TO CONTROLLER*

The Contracting Parties have concluded this Agreement based on model contractual clauses (hereinafter "model contractual clauses" or the "Agreement").

Data Exporter

Full Name: .....
[Data Exporter's name]

Address: .....
[Data Exporter's address]

Contact details: .....
[Data Exporter's contact details]

Governing law: .....
[Current data protection law of the country of the Data Exporter]

Competent Supervisory Authority: .....
[Data protection authority of the country of the Data Exporter]

Data Importer

Full name: .....
[Data Importer's name]

Address: .....
[Data Importer's address]

Contact details: .....
[Data Importer's contact details]

Signature Date: *Signed in [City, Country], on [MM/DD/YYYY],*

Data Exporter's Signature: .....

Data Importer's Signature: .....

MODEL AGREEMENT FOR THE INTERNATIONAL TRANSFER OF PERSONAL DATA FROM **CONTROLLERS TO CONTROLLERS**

The Contracting Parties have concluded this Agreement based on model contractual clauses:

FIRST PART:
GENERAL PROVISIONS

Clause 1.

Purpose, parties, scope of application, and definitions

1.1. Purpose

a. The purpose of these model contractual clauses is to ensure and facilitate compliance with the requirements for the international transfer of Personal Data set by the Governing Law, in order to comply with the principles and obligations for the protection of Personal Data and the rights of Data Subjects.

b. Any interpretation of this Agreement shall take these purposes into account.

1.2. Contracting parties

a. The Contracting Parties are the Data Exporter and the Data Importer.

b. This Agreement allows the incorporation of additional importers or exporters as Contracting Parties using the form in Annex A and following the procedure established in Clause 5.

1.3. Scope of application

a. This Agreement shall apply to international transfers of Personal Data between Data Exporters and Data Importers, in accordance with the specifications in Annex B.

b. The annexes form an integral part of this Agreement.

1.4. Definitions

a. The defined terms are identified in this Agreement by their capital letters.

b. For the purposes of this Agreement, the following terms shall be defined:

Agreement:
this contract for the international transfer of Personal Data based on model contractual clauses together with its title page and its annexes.

Anonymization:
the application of measures of any kind aimed at preventing the identification or re-identification of an individual without disproportionate efforts.

Competent Supervisory Authority:
Personal data protection authority in the country of the Data Exporter or Data Importer.

Cloud Computing:
model for enabling access to a set of IT services (such as networks, servers, storage, applications, and services) in a convenient manner and on demand, which can be rapidly provided and released with administrative efforts and based on the interaction with the service provider.

Consent:
expression of the free, specific, unequivocal and informed will of the Data Subject through which he/she accepts and authorizes the processing of his/her Personal Data.

Personal Data:
any information regarding an identified or identifiable individual, expressed in a numerical, alphabetical, graphical, photographic, alpha-numeric, or acoustic way, or in any other form. It is considered that a person is identifiable when his/her identity can be determined directly or indirectly, provided that this does not require disproportionate time or efforts.

Sensitive Personal Data:
Personal Data that refer to the intimate sphere of the Data Subject, the undue use of which may result in discrimination or create a serious risk thereof. In an illustrative way, Personal Data that may reveal aspects such as racial or ethnic origin; beliefs or religious, philosophical and moral convictions; trade union membership; political opinions; information regarding health, sexual life, preference or orientation; genetic data; or biometric data aimed at identifying a natural person in an unequivocal manner will be considered as sensitive.

Automated Individual Decisions:
decisions that produce legal effects concerning the Data Subject, or that affect him/her in a significant way, based solely on automated processing intended to assess, without human intervention, specific personal aspects, or to analyze or predict, specifically, his/her professional performance, economic situation, health status, sexual preferences, reliability or behavior.

Processor:
service provider who, as a natural or legal person or public authority, outside the organization of the Controller, processes Personal Data in the name and on behalf of the Controller.

Standards:
Standards for Personal Data Protection for the Ibero-American States approved by the RIPD in 2017.

Data Exporter:
natural person or private legal entity, public authority, service, body or service provider, located in the territory of a State, which performs international transfers of Personal Data, according to the provisions of the Standards.

Data Importer:
natural person or private legal entity, public authority, service, body or service provider located in a third country, that receives Personal Data from a Data Exporter through an international transfer of Personal Data.

Governing Law:
the Personal Data protection law of the Data Exporter's jurisdiction.

Administrative, Physical, and Technical Measures:
measures aimed at preventing any damage, loss, alteration, destruction, access to, and in general any illicit or unauthorized use of Personal Data, even if accidental, sufficient to ensure the confidentiality, integrity and availability of the Personal Data.

Controller:
natural person or private legal entity, public authority, service or body that, alone or together with others, determines the purposes, means, scope and other matters related to the Processing of Personal Data.

Sub-processor:
another Processor relied on by the Processor to carry out certain Processing activities on behalf of the Controller.

Third-Party Beneficiaries:
Data Subject whose Personal Data is subject to an international transfer under this Agreement. The Data Subject is a Third-Party Beneficiary of the rights provided in his/her favor in the MCCs, and can therefore exercise the rights granted to it by the MCCs, even if he/she has not joined the model contract between the Parties.

Data Subject:
natural person to whom the Personal Data relates.

Onward Transfer:
transfer of data by the Data Importer to a third party located outside of the jurisdiction of the Data Exporter that complies with the safeguards set out in the MCCs.

Processing:
any operation or set of operations performed on Personal Data through physical or automated procedures related, but not limited, to the collection, access, registration, organization, structuring, adaptation, indexation, modification, extraction, consultation, storage, conservation, elaboration, transfer, dissemination, possession, exploitation, and in general, any use or disposal of Personal Data.

Personal Data Breach:
any damage, loss, alteration, destruction, access, and in general any illicit or unauthorized use of Personal Data, even if accidental.

Clause 2.

Effects and invariability of the clauses

2.1. Modification of the model contractual clauses. Limitations

This Agreement based on model contractual clauses establishes adequate safeguards for Data Subjects pertaining to the transfer of their data, from Controller(s) to Controller(s), provided that the clauses are not modified in their essence compared to the original model, except to complete the title page and the annexes. This does not prevent the Parties from including model contractual clauses in a broader contract, nor does it prevent them from adding further clauses or safeguards, provided they do not directly or indirectly contradict these model contractual clauses or affect the rights of Data Subjects.

2.2. Hierarchy with the governing law. Interpretation

a. This Agreement shall be read and interpreted in accordance with the provisions of the Governing Law.

b. The Parties may add new definitions and further safeguards to these model contractual clauses when necessary to comply with the Governing Law and provided this does not negatively affect the protections granted by the model contractual clauses.

c. This Agreement shall not be interpreted in a manner that conflicts with the rights and obligations set out in the Governing Law.

d. This Agreement is understood to be without prejudice to the obligations to which the Data Exporter is subject by virtue of its legislation or the Governing Law.

2.3. Hierarchy with other agreements

In case of a contradiction between this Agreement and the provisions of related agreements between the Parties, the clauses of this Agreement shall prevail.

Clause 3.

Third-party beneficiaries

Data Subjects may invoke, as Third-Party Beneficiaries, the clauses of this Agreement against the Data Exporter and/or the Data Importer and require them to ensure compliance.

Clause 4.

Description of the transfer(s) and the purpose(s) thereof

The details and characteristics of the transfer or transfers and, particularly, the categories of the Personal Data transferred and the purposes for which they are transferred are specified in Annex B of this Agreement.

Clause 5.

Docking clause

a. The Parties accept that any entity that is not a party to this Agreement may, with the prior consent of all Parties involved, adhere to this Agreement at any time, either as a Data Exporter or as a Data Importer, by signing the form in Annex A, and completing the other Annexes, if applicable.

b. Once it has signed Annex A and completed the other annexes, if applicable, the joining entity shall be considered a Party to this Agreement and shall have the rights and obligations of a Data Exporter or a Data Importer, depending on the role under which it has adhered to the Agreement, as indicated in Annex A.

c. The entity joining the Agreement shall not acquire rights and obligations under this Agreement for the period prior to its adhesion.

SECOND II:
OBLIGATIONS OF THE PARTIES

Clause 6.

Data protection safeguards

6.1. Principle of accountability

a. The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able to perform its obligations under this Agreement by applying appropriate Administrative, Physical and Technical Measures.

b. The Data Importer shall implement the necessary mechanisms to demonstrate compliance with the principles and obligations established in this Agreement, thereby ensuring accountability to the Data Subject and the Competent Supervisory Authority for the Processing of the Personal Data in its possession.

c. The Data Importer shall review and permanently assess the mechanisms that it voluntarily adopts to comply with the principle of accountability, in order to measure their level of effectiveness in complying with this Agreement.

6.2. Principle of purpose limitation

a. The Data Importer shall not process the Personal Data subject to this Agreement for purposes other than those set out in Annex B.

b. It may only process Personal Data for other purposes: (i) with the prior consent of the Data Subject; (ii) when necessary for the establishment, exercise, or defense of legal claims within the framework of specific administrative, regulatory, or judicial procedures; (iii) when the Processing is necessary to protect the vital interests of the Data Subject or of another natural person.

6.3. Transparency

a. For Data Subjects to effectively exercise the rights granted to them by this Agreement, the Data Importer shall inform them of the following, either directly or through the Data Exporter: (i) its identity and contact details; (ii) the categories of Personal Data processed and their purposes; (iii) the right to request a copy of this Agreement free of charge; (iv) when it intends to carry out onward transfers of Personal Data to third parties, the recipient or categories of recipients and the purpose of such onward transfers.

b. This shall not apply when the Data Subject already has the information, or when it is impossible to communicate such information or if it requires disproportionate efforts from the Data Importer.

c. Where a copy of the Agreement is requested, the Parties may redact the sections or annexes of the Agreement that contain trade secrets or other types of confidential information, such as Personal Data of third parties or confidential information related to the contractual obligations between the Parties.

6.4. Data accuracy and minimization

a. The Parties shall ensure that the Personal Data is accurate and, where necessary, kept up to date. The Data Importer shall take all reasonable steps to promptly delete or rectify any Personal Data that is inaccurate for the purposes for which it is being processed.

b. If either Party becomes aware that the Personal Data transferred or received is inaccurate or outdated, it shall inform the other Party without undue delay.

c. The Data Importer shall ensure that the Personal Data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is being processed.

6.5. Storage limitation

a. The Data Importer shall retain the Personal Data for no longer than necessary for the purposes for which it is processed.

b. The Data Importer shall put in place appropriate Administrative, Physical, and Technical Measures to ensure compliance with this obligation, including the deletion or anonymization of the data and all back-ups at the end of the retention period.

6.6. Principle of data security

a. The Data Importer and, during the transfer, also the Data Exporter, shall implement and maintain appropriate Administrative, Physical and Technical Measures to ensure the confidentiality, integrity, and availability of the Personal Data subject to this Agreement.
To determine the security measures, the Data Importer shall consider the following factors:

i) the risk to the rights and freedoms of the Data Subjects, particularly due to the potential quantitative and qualitative value that the processed Personal Data could represent for a third party that is not authorized to possess it;
ii) the state of the art;
iii) the costs of implementation;
iv) the nature of the processed Personal Data, especially if it is Sensitive Personal Data;
v) the scope, context, and purposes of the Processing;
vi) the potential consequences of a Personal Data Breach for the Data Subjects;
vii) previous Personal Data Breaches that occurred in the Processing of the Personal Data.

b. The Parties have agreed to the Administrative, Physical and Technical Measures listed in Annex C to this Agreement for the Personal Data that are the subject of the international transfer.

c. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an adequate level of security.

Personal data breach

a. In the event of a Personal Data Breach of Personal Data processed by the Data Importer under this Agreement, the Data Importer shall take appropriate steps to address the breach and to mitigate any potential negative effects.

b. The Data Importer shall document all relevant facts related to the Personal Data Breach, such as its effects and the corrective measures taken, and keep a record thereof.

c. Whenever one of the Parties becomes aware of a Personal Data Breach, it shall notify the other Party, the Competent Supervisory Authority, and the affected Data Subjects thereof, without any delay and at the latest within a period of not more than five (5) days.

d. The notification set out in the previous paragraph shall be drafted in clear and simple language. Said notification shall at least contain the following information:

i) the nature of the incident;
ii) the affected Personal Data;
iii) the corrective measures immediately adopted;
iv) in the event of notification to the Data Subject, recommendations on the measures to be adopted by the latter to protect his/her interests;
v) the means available to the Data Subject to obtain more information

e. To the extent the Data Importer is unable to provide all information at once, it may do so in phases without further undue delay.

f. Data Subjects do not have to be notified when said notification involves disproportionate efforts. In this case, the Data Importer shall issue a public communication or take similar measures to inform the public of the Personal Data Breach.

6.7. Processing under the authority of the data importer and principle of confidentiality

a. The Data Importer shall ensure that any person acting under its authority processes the data in accordance with the instructions given by the Data Importer, and shall establish controls or mechanisms for those intervening in any phase of the Processing of the Personal Data to maintain and respect the confidentiality thereof, which is an obligation that shall continue to apply even after the end of its contractual relationship with the Data Exporter.

b. The Data Importer shall ensure that the persons authorized to process the Personal Data have agreed to respect the principle of confidentiality or are subject to a legal confidentiality obligation.

6.8. Processing of sensitive personal data

a. Where the transfer involves Sensitive Personal Data, the Data Importer shall apply specific restrictions and additional safeguards adapted to the specific nature of the data and the risk involved.

b. These measures may consist of, for example, restricting the personnel permitted to access the Personal Data, special confidentiality agreements, additional security measures (such as Anonymization), and/or additional restrictions related to Onward Transfers.

c. Where the transfer involves Personal Data concerning children or adolescents, the Parties shall privilege the protection of their superior interests, in accordance with the Convention on the Rights of the Child and other international instruments.

6.9. Onward Transfers

a. The Data Importer may only disclose the Personal Data to third parties located outside the Data Exporter's jurisdiction if the third party is or agrees to be bound by this Agreement. Otherwise, the Data Importer may only carry out an Onward Transfer in the following cases:

(i) in case this is provided for by the Governing Law, the Onward Transfer is to a country that has been the subject of an adequacy decision regarding its level of protection of Personal Data in accordance with the provisions of the Governing Law, provided that such decision covers the Onward Transfer;
(ii) the third party recipient of the Onward Transfer otherwise provides adequate safeguards, in accordance with the Governing law, with regard to Personal Data subject to the Onward Transfer;
(iii) the third party enters into a binding instrument with the Data Importer that ensures the same level of data protection as under this Agreement, and the Data Importer provides a copy of these safeguards to the Data Exporter;
(iv) the Onward Transfer is necessary for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings;
(v) if it is necessary to protect the vital interests of the Data Subject or of another natural person; or
(vi) where none of the other conditions applies, the Data Importer has obtained the explicit Consent of the Data Subject for an Onward Transfer in a specific situation, after having informed him/her of the purpose, the identity of the recipient, and the possible risks of such transfer to the Data Subject due to the lack of appropriate data protection safeguards. In this case, the Data Importer shall inform the Data Exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the Data Subject.

b. All Onward Transfers shall be subject to compliance by the Data Importer with the other safeguards provided in this Agreement and, in particular, compliance with the principle of purpose limitation.

6.10. Documentation and compliance

a. Each Party shall be able to demonstrate compliance with its obligations under this Agreement.

b. In particular, the Data Importer shall keep appropriate documentation of the processing activities carried out under its responsibility, which shall be made available upon request to the Data Exporter and, where appropriate, the Competent Supervisory Authority.

Clause 7.

Rights of data subjects

a. The Data Importer, where relevant with the assistance of the Data Exporter, shall deal with any enquiries and requests from a Data Subject relating to the Processing of their Personal Data and the exercise of their rights under this Agreement. It shall do so free of charge and without undue delay, and at the latest within a period of fifteen business days of their receipt, unless the applicable law indicates a shorter time,

b. The Data Importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of rights of Data Subjects. Any information provided to Data Subjects shall be in an intelligible and easily accessible form, using clear and plain language.

c. In particular, Data Subjects shall have the right:

(i) to request confirmation on the processing of their Personal Data, to access their Personal Data in the possession of the Data Importer, including to obtain a complete copy thereof, as well as to be informed about the general and specific conditions of the Processing, including information about the categories of Personal Data processed, the purpose of the Processing, the retention period (or the criteria to determine it), the existence of any Onward Transfers, including the recipients and the purposes thereof, and information about the right to file a complaint with the Competent Supervisory Authority;
(ii) to request the Data Importer to rectify or correct any inaccurate, incomplete or outdated Personal Data;
(iii) to request the destruction or deletion of their Personal Data from the Data Importer's files, records and systems, so that they are no longer in its possession and cease to be processed, when the data is processed in violation of their Third-Party Beneficiaries rights arising from this Agreement, or when the Data Subject withdraws his/her consent to the Processing;
(iv) to object to the Processing of their Personal Data for direct marketing purposes, including profiling, to the extent that it is related to such activity.
(v) to request and access the Agreement entered into between the Data Importer and the Data Exporter, following redaction of any confidential information related to third parties and to the extent this is in line with the rules applicable to the Data Importer.

7.1 Limitations on the exercise of the rights of the data subject

a. The Data Importer may refuse a Data Subject's request where permitted under the laws of the country of destination and when necessary and proportionate in a democratic society to protect important objectives of general public interest or the rights and freedoms of individuals.

b. If the Data Importer intends to refuse a Data Subject's request, it shall inform him/her of the reasons for the refusal and of the possibility of lodging a complaint with the Competent Supervisory Authority or of seeking judicial redress.

7.2 Right not to be subject to automated individual decisions

a. The Data Importer shall not make any Automated Individual Decision with respect to the transferred Personal Data.

b. The prohibition according to the preceding paragraph shall not apply when (i) the Automated Individual Decision is authorized by the laws of the Data Importer's country, which ensures appropriate safeguards for the rights of Data Subjects, or (ii) the Automated Individual Decision is based on the Data Subject's explicit consent.

c. When the data processing is authorized by law or the Data Subject has given his/her consent, the Data Subject shall have the right to (i) receive an explanation about the decision made; (ii) be heard and express his/her point of view and challenge the decision, and (iii) obtain a human intervention.

d. The Controller may not carry out automated Personal Data Processing that leads to discrimination against Data Subjects due to their racial or ethnic origins; religious, philosophical, and moral beliefs or convictions; trade union membership; political opinions; sexual life, preference or orientation; or the Processing of health, genetic or biometric data.

Clause 8.

Redress

a. The Data Importer shall inform the Data Subjects, in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints, which shall handle complaints received from the Data Subjects as quickly as possible [**OPTION:** The Data Importer agrees that Data Subjects may also lodge a complaint with an independent dispute resolution body at no cost. The Data Importer shall inform the Data Subjects of this redress mechanism, in the manner established in this paragraph, and that they are not required to use this mechanism or follow a particular sequence in seeking redress.]

b. In case of a dispute between a Data Subject and one of the Parties as regards compliance with this Agreement, 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, collaborate in good faith in resolving them.

c. Whenever a Data Subject invokes a Third-Party Beneficiary Right under this Agreement, the Data Importer undertakes to accept and not dispute the Data Subject's decision to: (i) lodge a complaint with the Supervisory Authority in its country of habitual residence or place of work, or with the Competent Supervisory Authority; (ii) bring legal proceedings regarding their Personal Data in accordance with the provisions of Clause 14 of this Agreement.

d. The Data Importer agrees to abide by decisions that are binding under the Governing Law or other applicable law.

Clause 9.

Civil liability

a. Each Party shall be liable to the other Party for any damage caused by any breach of the rights and obligations set out in this Agreement.

b. Each Party shall be liable to the Data Subject. The Data Subject shall be entitled to receive compensation for any material or non-material damages caused by any of the Parties for violating the Third-Party Beneficiary Rights under this Agreement. This is without prejudice to the liability of the Data Exporter under the Governing Law.

c. Where more than one Party is responsible for any damage or loss caused to the Data Subject as a result of a breach of this Agreement, all responsible Parties shall be jointly and severally liable.

d. The Parties agree that if one Party is held liable under the previous paragraph, 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 or loss caused.

Clause 10.

Supervision by the competent supervisory authority

a. 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 this Agreement.

b. In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the Supervisory Authority, especially the remedial and compensatory measures. It shall provide the Supervisory Authority with a written confirmation that the necessary measures have been taken.

c. Similarly, the Data Importer agrees to submit itself to the powers of the Competent Supervisory Authority in relation to the suspension of transfers, the suspension of contracts, and any other measures that the Supervisory Authority may require.

Clause 11.

Local laws and practices affecting compliance with the clauses

a. The Parties confirm that, at the time of entering into this Agreement, they have used reasonable efforts to identify whether the transferred data is covered by any local law or practice in the Data Importer's jurisdiction that goes beyond what is necessary and proportionate in a democratic society to safeguard important public interest objectives, and that may reasonably be expected to affect the protections, rights, and safeguards afforded to Data Subjects under this Agreement. Based on the foregoing, the Parties confirm that they are not aware of the existence of any practice or norm that could adversely affect the specific safeguards under this Agreement.

b. The Data Importer agrees to notify immediately the Data Exporter if any such laws become applicable to it in the future. If such notification is made, or if the Data Exporter has a reason to believe that the Data Importer is no longer able to perform its obligations under this Agreement, the Data Exporter shall identify appropriate measures to address the situation (for example, Administrative, Physical and Technical Measures to ensure the security of the data).

c. Similarly, the Data Exporter may suspend transfers under this Agreement if it considers that adequate safeguards cannot be ensured. In this case, the Data Exporter shall have the right to terminate this Agreement in accordance with the conditions set out in Clause 12.

d. If a court or government agency requires the Data Importer to disclose or use the transferred data in a manner not otherwise permitted by this Agreement, the Data Importer shall assess the legality of such request and challenge it if, following a careful legal assessment, it concludes that there are reasonable grounds to believe that the request is illegal under local law and affects the rights ensured by this Agreement. Where permitted by local law, it shall also promptly notify the Data Exporter that it has received such request. If the Data Importer is prohibited by local law from notifying the Data Exporter, the Data Importer shall use reasonable efforts to obtain a waiver of such prohibition.

SECTION III:
FINAL PROVISIONS

Clause 12.

Non-compliance with the clauses and termination

a. The Data Importer shall immediately notify the Data Exporter if it is unable to comply with any provision of this Agreement, for whatever reason.

b. In the event that the Data Importer fails to comply with its obligations under this Agreement, the Data Exporter shall suspend the transfer of Personal Data to the Data Importer until compliance is again ensured or the contract is terminated.

c. The Data Exporter shall be entitled to terminate this Agreement when:

(i) the Data Exporter has suspended the transfer of Personal Data to the Data Importer pursuant to the previous paragraph and compliance with this Agreement is not restored within a reasonable period of time and in any event within thirty (30) business days from the suspension;

(ii) the Data Importer is in substantial or persistent breach of this Agreement; or

(iii) the Data Importer fails to comply with a binding decision of a competent court or Supervisory Authority regarding its obligations under this Agreement. In this case, it shall inform the competent Supervisory Authority of its non-compliance.

d. Personal Data that has been transferred prior to the termination of the contract pursuant to the previous paragraph 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 this Agreement. 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 this Agreement and will only process the data to the extent and for as long as required under that local law.

Clause 13.

Governing law

This Agreement shall be governed by the Governing Law.

Clause 14.

Choice of forum and jurisdiction

a. Any dispute arising from this Agreement shall be resolved by the courts of the Data Exporter's jurisdiction.

b. Data Subjects may also bring legal proceedings against the Data Exporter and/or the Data Importer, which may be initiated, at the Data Subject's choice, in the country of the Data Exporter or in which the Data Subject has his/her habitual residence. With respect to the Data Importer, s/he may also file legal proceedings in the country of the Data Importer.

c. The Parties agree to submit to the competent court(s) provided for in this clause.

ANNEXES

ANNEX A
ACCESSION FORM FOR NEW PARTIES

ANNEX B
DESCRIPTION OF THE TRANSFER

ANNEX C
ADMINISTRATIVE, PHYSICAL AND TECHNICAL MEASURES TO ENSURE DATA SECURITY

ANNEX A

ACCESSION FORMS FOR NEW PARTIES

Data Exporter Accession

Full name: .....
[Data Exporter's Name]

Address: .....
[Data Exporter's Address]

Contact details: .....
[Data Exporter's Contact details]

Activities related to the data transferred under this Agreement: .....
[...]

Governing Law: .....
[Current data protection law of the Data Exporting country]

Competent Supervisory Authority: .....
[Data protection authority of the country of the Data Exporter]

Data Importer Accession

Full name: .....
[Data Importer's Name]

Address: .....
[Data Importer's Address]

Contact details: .....
[Data Importer's Contact details]

Signature Date: Signed in *[City, Country]*, on *[MM/DD/YYYY]*

Data Exporter's Signature:

X .....

Data Importer's Signature:

X .....

Consent of the Parties: *[.....]*

ANNEX B

DESCRIPTION OF THE TRANSFER

Categories of Data Subjects whose Personal Data is transferred: *[...]*

.....

Categories of Personal Data transferred: *[...]*

.....

Sensitive Personal Data transferred (if applicable) and restrictions or safeguards applied: *[...]*

.....

Transfer Frequency: .....

[for example, if the data is transferred all at once or periodically].

Purpose(s) of the data transfer and further processing *[...]*

Retention period:

[period during which the Personal Data shall be kept or, when this is not possible, the criteria used to determine this period].

ANNEX C

ADMINISTRATIVE, PHYSICAL AND TECHNICAL MEASURES TO ENSURE DATA SECURITY

NOTE: [In this Annex C, the Parties must set out in detail the specific Administrative, Physical and Technical Measures that they agree on in order to ensure the security of the data transferred under this Agreement. Examples of such measures include, but are not limited to, measures to anonymize and encrypt Personal Data, measures to ensure the permanent confidentiality, integrity, availability and resilience of processing systems and services, measures to restore availability and access to Personal Data quickly in the event of a physical or technical incident, regular verification, evaluation and assessment of the effectiveness of the Administrative, Physical and Technical Measures to ensure the security of data processing, measures for the identification and authorization of users, measures for the protection of data during transmission, measures for the protection of data during storage, measures to ensure the physical security of the premises where the Personal Data is processed, measures to ensure the recording of incidents, measures to ensure system settings, especially default settings, internal information technology and security governance and management measures, measures for the certification/warranty of processes and products, measures to ensure data minimization, measures to ensure the quality of the data, measures to ensure proactive responsibility, and measures to ensure limited data retention. This statement does not replace the actual specification of the Administrative, Physical and Technical Measures to be adopted and implemented by the Parties. Administrative, Physical and Technical Measures must be described specifically and not in a generic way].

ANNEX D

ADDITIONAL LEGAL DOCUMENTATION

[This section must include the documents that the rules applicable to the Parties consider mandatory for the Processing of Personal Data, such as privacy notices or privacy policies].

2.

MODEL AGREEMENT FOR THE INTERNATIONAL TRANSFER OF PERSONAL DATA *CONTROLLERS AND PROCESSORS*

The Parties to the Contract have agreed to this Agreement based on model contract clauses (hereinafter, "model contract clauses" el "Agreement").

Data Exporter

Full name: .....
[Data Exporter's Name]

Address: .....
[Data Exporter's Address]

Contact details: .....
[Data Exporter's Contact details]

Applicable Law: .....
[Current data protection law of the Data Exporting country]

Competent supervisory authority: .....
[Personal Data Protection Authority of the Data Exporter's country]

Data Importer

Full name: .....
[Data Importer's Name]

Address: .....
[Data Importer's Address]

Contact details: .....
[Data Importer's Contact details]

Signature Date: Signed in *[City, Country]*, on *[MM/DD/YYYY]*

Data Exporter's Signature:

X .....

Data Importer's Signature:

X .....

The Contracting Parties have concluded this Agreement based on model contractual clauses:

FIRST PART:
GENERAL PROVISIONS

Clause 1.

Purpose, parties, scope of application and definitions

1.1. Purpose

a. The purpose of these model contractual clauses is to ensure and facilitate compliance with the requirements for the international transfer of Personal Data set by the Governing Law, in order to comply with the principles and obligations on the protection of Personal Data

b. Any interpretation of this Agreement shall take these purposes into account.

1.2. Contracting parties

a. The Contracting Parties are the Data Exporter and the Data Importer

b This Agreement allows the incorporation of additional importers or exporters as Contracting Parties, using the form in Annex A following the procedure established in Clause 5.

1.3. Scope of application

This Agreement shall apply to international transfers of Personal Data between Data Exporters and Data Importers, in accordance with the specifications of Annex B. The annexes form an integral part of this Agreement.

The defined terms are identified in this Agreement by capital letters. For the purposes of this Agreement, the following terms shall be defined:

Agreement:
this contract for the international transfer of Personal Data based on model contractual clauses together with its title page and its annexes.

Anonymization:
the application of measures of any kind aimed at preventing the identification or re-identification of an individual without disproportionate efforts.

Competent Supervisory Authority:
personal data protection authority in the country of the Data Exporter or Data Importer.

Cloud Computing:
model for enabling access to a set of IT services (such as networks, servers, storage, applications, and services) in a convenient manner and on demand, which can be rapidly provided and released with administrative efforts and based on the interaction with the service provider.

Consent:
expression of the free, specific, unequivocal and informed will of the Data Subject through which he/she accepts and authorizes the Processing of his/her Personal Data.

Personal Data:
any information regarding an identified or identifiable individual, expressed in a numerical, alphabetical, graphical, photographic, alpha-numeric, oracoustic way, or in any other form. It is considered that a person is identifiable when his/her identity can be determined directly or indirectly, provided that this does not require disproportionate time or efforts.

Sensitive Personal Data:
Personal Data that refer to the intimate sphere of the Data Subject, the undue use of which may result in discrimination or create a serious risk thereof. In an illustrative way, Personal Data that may reveal aspects such as racial or ethnic origin; beliefs or religious, philosophical and moral convictions; trade union membership; political opinions; information regarding health, sexual life, preference or orientation; genetic data; or biometric data aimed at identifying a natural person in an unequivocal manner will be considered as sensitive.

Automated Individual Decisions:
decisions that produce legal effects concerning the Data Subject, or that affect him/her in a significant way, based solely on automated processing intended to assess, without human intervention, specific personal aspects, or to analyze or predict, specifically, his/her professional performance, economic situation, health status, sexual preferences, reliability or behavior.

Processor:
service provider who, as a natural or legal person or public authority, outside the organization of the Controller, processes Personal Data in the name and on behalf of the Controller.

Standards:
Standards for Personal Data Protection for the Ibero-American States approved by the RIPD in 2017.

Data Exporter:
natural person or private legal entity, public authority, service, body or service provider, located in the territory of a State that performs international transfers of Personal Data, according to the provisions of the Standards.

Data Importer:
natural person or private legal entity, public authority, service, body or service provider located in a third country that receives Personal Data from a Data Exporter through an international transfer of Personal Data.

Governing Law:
the Personal Data protection law of the Data Exporter's jurisdiction.

Administrative, Physical and Technical Measures:
measures aimed at preventing any damage, loss, alteration, destruction, access, and, in general, any illicit or unauthorized use of Personal Data, even if accidental, sufficient to ensure the confidentiality, integrity and availability of the Personal Data.

Controller:
natural person or private legal entity, public authority, service or body that, alone or together with others, determines the purposes, means, scope and other matters related to the Processing of Personal Data.

Sub-processor:
another Processor relied on by the Processor to carry out certain processing activities on behalf of the Controller.

Third-Party Beneficiaries:
Data Subject whose Personal Data is subject to an international transfer under this Agreement. The Data Subject is a Third-Party Beneficiary of the rights provided in his/her favor in the MCCs and can therefore exercise the rights granted to it by the MCCs, even if s/he has not joined the model contract between the Parties.

Data Subject:
natural person to whom the Personal Data relates.

Onward Transfer:
transfer of data by the Data Importer to a third party located outside of the jurisdiction of the Data Exporter that complies with the safeguards set out in the MCCs.

Processing:
any operation or set of operations performed on Personal Data through physical or automated procedures, related, but not limited, to the collection, access, registration, organization, structuring, adaptation, indexation, modification, extraction, consultation, storage, conservation, elaboration, transfer, dissemination, possession, exploitation, and in general any use or disposal of Personal Data.

Personal Data Breach:
any damage, loss, alteration, destruction, access, and in general any illicit or unauthorized use of Personal Data, even if accidental.

Clause 2.

Effects and invariability of the clauses

2.1. Modification of the model contractual clauses. Limitations

This Agreement based on model contractual clauses establishes adequate safeguards for Data Subjects pertaining to the transfer of their data, from Controller(s) to Processor(s), provided that the clauses are not modified in their essence compared to the original model, except to complete the title page and the annexes. This does not prevent the Parties from including model contractual clauses in a broader contract, nor does it prevent them from adding further clauses or safeguards, provided they do not directly or indirectly contradict these model contractual clauses or affect the rights of Data Subjects.

2.2. Hierarchy with the governing law. Interpretation

a. This Agreement shall be read and interpreted in accordance with the provisions of the Governing Law.

b. The Parties may add new definitions and further safeguards to these model contractual clauses when necessary to comply with the Governing Law and provided this does not negatively affect the protections granted by the model contractual clauses.

c. This Agreement shall not be interpreted in a manner that conflicts with the rights and obligations set out in the Governing Law.

d. This Agreement is understood to be without prejudice to the obligations to which the Data Exporter is subject by virtue of its legislation or the Governing Law.

2.3. Hierarchy with other agreements

In case of a contradiction between this Agreement and the provisions of related agreements between the Parties, the clauses of this Agreement shall prevail.

Clause 3.

Third-party beneficiaries

Data Subjects may invoke, as Third-Party Beneficiaries, the clauses of this Agreement against the Data Exporter and/or the Data Importer and require them to ensure compliance.

Clause 4.

Description of the transfer(s) and the purpose(s) thereof

The details and characteristics of the transfer or transfers and, particularly, the categories of the Personal Data transferred and the purposes for which they are transferred are specified in Annex B of this Agreement.

Clause 5.

Docking clause

a. The Parties accept that any entity that is not a Party to this Agreement may, with the prior consent of all Parties involved, adhere to this Agreement at any time, either as a Data Exporter or as a Data Importer, by signing the form in Annex A, and completing the other Annexes, if applicable.

b. Once it has signed Annex A and completed the other annexes, if applicable, the joining entity shall be considered a Party to this Agreement and shall have the rights and obligations of a Data Exporter or a Data Importer, depending on the role under which it has adhered to the Agreement, as indicated in Annex A.

c. The entity joining the Agreement shall not acquire rights and obligations under this Agreement for the period prior to its adhesion.

SECTION II:
OBLIGATIONS OF THE PARTIES

Clause 6.

Data protection safeguards

6.1. Instructions

The Data Importer shall carry out Personal Data processing activities without any decision-making power over the scope and content thereof, and instead limit its actions to the terms and instructions established by the Data Exporter.

6.2. Principle of accountability

a. The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able to perform its obligations under this Agreement by applying appropriate Administrative, Physical and Technical Measures.

b. The Data Importer shall implement the necessary mechanisms to demonstrate compliance with the principles and obligations established in this Agreement, thereby ensuring accountability to the Data Subject and the Competent Supervisory Authority for the Processing of the Personal Data in its possession.

c. The Data Importer shall review and permanently assess the mechanisms that it voluntarily adopts to comply with the principle of accountability, in order to measure their level of effectiveness in complying with this Agreement.

6.3. Principle of purpose limitation

The Data Importer shall not process the Personal Data subject to this Agreement for purposes other than those set out in Annex B, unless instructed otherwise by the Data Exporter.

6.4. Transparency

a. Upon request, the Parties shall make a copy of this Agreement available to the Data Subject free of charge. In any case, the Data Importer shall proactively assume the responsibility to inform about its existence. The sections or annexes of the Agreement containing trade secrets or other types of confidential information such as Personal Data of third parties or confidential information related to the contractual obligations between the Parties may be redacted.

b. This clause is without prejudice to the obligations imposed upon the Data Exporter by the Governing Law.

6.5. Data accuracy and minimization

a. 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.

b. In this case, the Data Importer shall cooperate with the Data Exporter to erase or rectify the data.

6.6. Principle of data security

a. The Data Importer and, during the transfer, also the Data Exporter, shall implement and maintain appropriate Administrative, Physical and Technical Measures to ensure the confidentiality, integrity and availability of the Personal Data subject to this Agreement, including protection against Personal Data Breaches. In assessing the appropriate level of security, the parties shall duly consider the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, and the risks for the Data Subjects linked to the Processing. To comply with the obligations set out in this paragraph, the Data Importer shall implement, at least, the Administrative, Physical and Technical Measures listed in Annex C to this Agreement. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. In the event of a breach of the Personal Data processed by the Data Importer under this Agreement, the Data Importer shall take appropriate measures to address this breach, including measures to mitigate its adverse effects.

c. The Data Importer shall also notify the Data Exporter within seventy-two (72) hours of becoming aware of the Personal Data Breach. Such notification shall include a description of the Personal Data Breach (including, where possible, the categories of Personal Data and approximate number of Data Subjects affected), its likely consequences, and the measures taken or proposed to address the breach and especially, where appropriate, measures to mitigate its potential adverse effects.

d. 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.

e. The Data Importer shall cooperate with and assist the Data Exporter in enabling it to comply with its obligations under the Governing Law, in particular to notify the Competent Supervisory Authority and the affected Data Subjects, taking into account the nature of the Processing and the information available to the Data Importer.

6.7. Processing under the authority of the data importer and principle of confidentiality

a. The Data Importer shall ensure that the persons acting under its authority only process data in accordance with its instructions and 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 this Agreement.

b. The Data Importer shall ensure that the persons authorized to process the Personal Data maintain and respect the confidentiality thereof, which is an obligation that shall continue to apply even after the end of its contractual relationship with the Data Exporter.

6.8. Processing of sensitive personal data

a. Where the transfer involves Sensitive Personal Data, the Data Importer shall apply the specific restrictions and/or additional safeguards described in Annex C to this Agreement.

b. Where the transfer involves Personal Data concerning children or adolescents, the Data Importer shall privilege the protection of their superior interests, in accordance with the Convention on the Rights of the Child and other international instruments.

6.9. Onward transfers

a. The Data Importer shall only disclose Personal Data to a third party on documented instructions from the Data Exporter.

b. In addition, the Data Importer may only disclose the Personal Data to third parties located outside the Data Exporter's jurisdiction if the third party is bound by or agrees to be bound by this Agreement. Otherwise, the Data Importer may only carry out an Onward Transfer in the following cases:

(i) in case this is provided for in the Governing Law, the Onward Transfer is to a country that has been the subject of an adequacy decision regarding its level of protection of Personal Data in accordance with the provisions of the Governing Law, provided that such decision covers the Onward Transfer;

(ii) the third party recipient of the Onward Transfer otherwise provides adequate safeguards, in accordance with the Governing law, with regard to Personal Data subject to the Onward Transfer;

(iii) the Onward Transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(iv) if it is necessary to protect the vital interests of the Data Subject or of another natural person.

c. All Onward Transfers shall be subject to compliance by the Data Importer with the other safeguards provided in this Agreement and, in particular, compliance with the principle of purpose limitation.

6.10. Documentation and compliance

a. The Parties shall be able to demonstrate compliance with their obligations under this Agreement. In particular, the Data Importer shall keep appropriate documentation of the processing activities carried out under the instructions of the Data Exporter, which shall be made available to the Data Exporter and the Competent Supervisory Authority upon request.

b. The Data Importer shall promptly and in an appropriate manner deal with the Data Exporter's enquiries that relate to the Processing under this Agreement.

c. The Data Importer shall make available to the Data Exporter all information necessary to demonstrate compliance with the obligations set out in this Agreement and, at the Data Exporter's request, allow for and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals or if there are indications of non-compliance. The Data Exporter may choose to conduct the audit by itself or mandate an independent auditor to do so. Audits may include inspections at the premises or physical facilities of the Data Importer and shall, where appropriate, be carried out with reasonable notice.

d. The Parties shall make the information referred to in the previous paragraphs, including the results of any audits, available to the Competent Supervisory Authority upon request.

6.11. Duration of the data processing and deletion or return of the data

a. Processing by the Data Importer shall only take place for the duration specified in Annex B to this Agreement.

b. After the end of the provision of the processing services, the Data Importer shall, at the request of the Data Exporter, securely 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 and securely delete existing copies, should the Data Exporter choose the latter option.

c. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with this Agreement. 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 this Agreement and will only process the data to the extent and for as long as required under that local law.

Clause 7.

Reliance on sub-processors

7.1. Sub-processor authorization form

[**OPTION 1**: SPECIFIC PRIOR AUTHORISATION]:

a. The Data Importer may only sub-contract the processing activities it performs on behalf of the Data Exporter under this Agreement to a Sub-processor with the Data Exporter's prior specific written authorization. The Data Importer shall submit the request for specific authorization at least within 15 business days prior to the engagement of the Sub-processor, together with the information necessary to enable the Data Exporter to decide on the authorization. The list of Sub-processors already authorized by the Data Exporter can be found in Annex D to this Agreement. The Parties shall keep Annex D up to date.

[**OPTION 2**: GENERAL WRITTEN AUTHORISATION]:

a. The Data Importer has the Data Exporter's general authorization to contract the Sub-processors included in the 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 15 business days 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) in question. The Data Importer shall provide the Data Exporter with the information necessary to enable the Data Exporter to exercise its right to object.

7.2. Data sub-processor agreement

a. 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 this Agreement, including in terms of Third-Party Beneficiary rights for Data Subjects. The Parties agree that, by complying with this provision, the Data Importer fulfils its obligations under the clause on Onward Transfers. The Data Importer shall ensure that the Sub-processor complies with the obligations to which it is subject pursuant to this Agreement.

b. The Data Importer shall provide the Data Exporter, at the latter's request, with a copy of the Sub-processor agreement and any subsequent amendments thereto. 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 thereof.

c. The Data Importer shall remain fully responsible to the Data Exporter for the performance of the Sub-processor's obligations under its agreement with the Data Importer. The Data Importer shall notify the Data Exporter of any failure by the Sub-processor to fulfil its obligations under that agreement.

Clause 8.

Rights of data subjects

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 such a request itself unless it has been authorized 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 in the exercise of their rights under the Governing Law. In this regard, the Parties shall set out in Annex C the appropriate Administrative, Physical and Technical Measures, taking into account the nature of the Processing, by which they ensure the assistance to the Data Exporter, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under the previous paragraphs, the Data Importer shall comply with the instructions from the Data Exporter.

Clause 9.

Redress

a. The Data Importer shall inform the Data Subjects, in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints, who shall handle the complaints received from Data Subjects as quickly as possible. [**OPTION:** The Data Importer agrees that the Data Subjects may also lodge a complaint with an independent dispute resolution body, at no cost to the Data Subjects. The Data Importer shall inform the Data Subjects of this redress mechanism, in the manner set out in this paragraph, and that they are not required to use it or follow a particular sequence in seeking redress.]

b. In case of a dispute between a Data Subject and one of the Parties as regards compliance with this Agreement, 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, collaborate in good faith to resolve them.

c. Whenever a Data Subject invokes a Third-Party Beneficiary Right under this Agreement, the Data Importer undertakes to accept and not dispute the Data Subject's decision to: (i) lodge a complaint with the Supervisory Authority in his/her country of habitual residence or place of work, or with the Competent Supervisory Authority; (ii) file an action in court as regards his/her Personal Data.

d. The Data Importer agrees to abide by decisions binding under the Governing Law or other applicable law.

Clause 10.

Civil liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of this Agreement.

b. Each Party shall be liable to the Data Subject. The Data Subject shall be entitled to receive compensation for any material or non-material damages caused by the Data Importer or its Sub-processor for violating the Third-Party Beneficiary Rights under this Agreement. This is without prejudice to the liability of the Data Exporter under the Governing Law.

c. The Parties agree that if the Data Exporter is held liable under the previous paragraph 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.

d. Where more than one Party is responsible for any damage caused to the Data Subject as a result of a breach of this Agreement, all responsible Parties shall be jointly and severally liable.

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

f. The Data Importer may not invoke the conduct of a Sub-processor to avoid its own liability.

Clause 11.

Supervision by the competent supervisory authority

a. 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 this Agreement.

b. In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the Supervisory Authority, especially corrective and compensatory measures. It shall provide the Supervisory Authority with a written confirmation that the necessary measures have been taken.

Clause 12.

Local laws and practices affecting compliance with the clauses

a. The Parties confirm that, at the time of entering into this Agreement, they have used reasonable efforts to identify whether the transferred data is covered by any local law or practice in the Data Importer's jurisdiction that goes beyond what is necessary and proportionate in a democratic society to safeguard important public interest objectives, and that may reasonably be expected to affect the safeguards, rights, and guarantees afforded to the Data Subject under this Agreement. Based on the foregoing, the Parties confirm that they are not aware of the existence of any such practice or rule that adversely affects the specific safeguards under this Agreement.

b. The Data Importer agrees to notify immediately the Data Exporter if any such laws become applicable to it in the future. In the event of such notification, or if the Data Exporter has reasons to believe that the Data Importer is no longer able to perform its obligations under this Agreement, the Data Exporter shall identify appropriate measures to address the situation (for example, Administrative, Physical and Technical Measures to ensure the security of the data). Likewise, it may suspend transfers under this Agreement if it considers that adequate safeguards cannot be ensured. In this case, the Data Exporter shall have the right to terminate this Agreement in accordance with the conditions set out in Clause 13.

c. If a court or government agency requires the Data Importer to disclose or use the transferred data in a manner not otherwise permitted by this Agreement, the Data Importer shall assess the legality of such request and challenge it if, after a careful legal assessment, it concludes that there are reasonable grounds to consider that the request is illegal under local law and that the request affects the rights guaranteed by this Agreement. To the extent permitted by local law, it shall also promptly notify the Data Exporter that it has received such a request. If the Data Importer is prohibited by local law from notifying the Data Exporter, the Data Importer shall use reasonable efforts to obtain a waiver of this prohibition.

SECTION III:
FINAL PROVISIONS

Clause 13.

Non-compliance with the clauses and termination

a. The Data Importer shall immediately notify the Data Exporter if it is unable to comply with any provision of this Agreement, for whatever reason.

b. In the event that the Data Importer fails to comply with its obligations under this Agreement, the Data Exporter shall suspend the transfer of Personal Data to the Data Importer until compliance is again ensured or the contract is terminated.

c. The Data Exporter shall be entitled to terminate this Agreement when:

(i) the Data Exporter has suspended the transfer of Personal Data to the Data Importer pursuant to the previous paragraph and compliance with this Agreement is not restored within a reasonable period of time and in any event within a period of thirty (30) business days following suspension;
(ii) the Data Importer is in substantial or persistent breach of this Agreement; or
(iii) the Data Importer fails to comply with a binding decision of a court or Competent Supervisory Authority regarding its obligations under this Agreement. In this case, it shall inform the Competent Supervisory Authority of its non-compliance.

d. Personal Data that has been transferred prior to the termination of the contract pursuant to the previous paragraph 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 this Agreement. 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 this Agreement and will only process the data to the extent and for as long as required under that local law.

Clause 14.

Governing law

This Agreement shall be governed by the Governing Law.

Clause 15.

Choice of forum and jurisdiction

a. Any dispute arising from this Agreement shall be resolved by the courts of the Data Exporter's jurisdiction.

b. Data Subjects may also bring legal action in court against the Data Exporter and/or the Data Importer, which may be initiated, at the Data Subject's choice, in the country of the Data Exporter, or in which the Data Subject has his/her habitual residence. With respect to the Data Importer, s/he may also bring legal action in the country of the Data Importer.

c. The Parties agree to submit to the competent court(s) provided for in this clause.

ANNEXES

ANNEX A
ACCESSION FORM FOR NEW PARTIES

ANNEX B
DESCRIPTION OF THE TRANSFER

ANNEX C
ADMINISTRATIVE, PHYSICAL AND TECHNICAL MEASURES
TO ENSURE DATA SECURITY

ANNEX D
LIST OF DATA SUBPROCESSORS

ANNEX A

ACCESSION FORM FOR NEW PARTIES

Data Exporter Accession

Full name: .....
[Data Exporter's Name]

Address: .....
[Data Exporter's Address]

Contact details: .....
[Data Exporter's contact details]

Activities related to the data transferred under this Agreement: .....
[...]

Governing Law: .....
[Current data protection law of the country of the Data Exporting]

Competent Supervisory Authority:.....
[Data protection authority of the country of the Data Exporter]

Jurisdiction: Courts of .....
[Data Exporter's domicile]

Data Importer Accession

Full name: .....
[Importer's Name]

Address: .....
[Importer's Address]

Contact details: .....
[Importer's Contact details]

Signature Date: Signed in *[City, Country]*, **on** *[MM/DD/YYYY]*

Data Exporter's Signature:

X .....

Data Importer's Signature

X .....

Consent of the Parties: *[.....]*

ANNEX B

DESCRIPTION OF THE TRANSFER

Categories of Data Subjects whose Personal Data is transferred: *[...]*

.....

Categories of Personal Data transferred: *[...]*

.....

Sensitive Personal Data transferred (if applicable) and restrictions or safeguards applied: *[...]*

Transfer Frequency: .....
[for example, if the data is transferred all at once or periodically].

Purpose(s) of the data transfer and further processing *[...]*

Term: .....
[period during which the Personal Data shall be kept or, when this is not possible, the criteria used to determine this period]

Sub-processors: .....
[in case of transfer to (Sub)processors, also specify the purpose, nature, and duration of the processing]

ANNEX C

ADMINISTRATIVE, PHYSICAL AND TECHNICAL MEASURES TO ENSURE DATA SECURITY

NOTE: [In this Annex C, the parties must set out in detail the specific Administrative, Physical and Technical Measures that they agree on in order to ensure the security of the data transferred under this Agreement. Examples of such measures include, but are not limited to, measures to anonymize and encrypt Personal Data, measures to ensure the permanent confidentiality, integrity, availability and resilience of processing systems and services, measures to restore availability and access to Personal Data quickly in the event of a physical or technical incident, regular verification, evaluation and assessment of the effectiveness of the Administrative, Physical and Technical Measures to ensure the security of data processing, measures for the identification and authorization of users, measures for the protection of data during the transfer, measures for the protection of data during storage, measures to ensure the physical security of the premises where the Personal Data is processed, measures to ensure the recording of incidents, measures to ensure system settings, especially default settings, internal information technology and security governance and management measures, measures for the certification/warranty of processes and products, measures to ensure data minimization, measures to ensure the quality of the data, measures to ensure proactive responsibility, and measures to ensure limited data retention. This statement does not replace the actual specification of the Administrative, Physical and Technical Measures to be adopted and implemented by the Parties. Administrative, Physical and Technical Measures must be described specifically and not in a generic way].

ANNEX D

LIST OF DATA SUBPROCESSORS

The Controller has authorized the use of the following Sub-processors:

Name/company name (denomination): *[...]*

Address: *[...]*

Name, position, and contact details: *[...]*

Description of data processing (including a well-defined delimitation of the responsibilities if several Sub-processors are authorized)**:** *[...]*

ANNEX E

ADDITIONAL LEGAL DOCUMENTATION

[This section must include the documents that the rules applicable to the Parties consider mandatory for the processing of Personal Data, such as privacy notices or privacy policies].