Agreement for the International Transfer of Personal Data

for the purpose of

Akamai service provisioning

and cyberthreat intelligence development and management

This agreement for the international transfer of personal data is entered into by and between **the entity with a registered seat in Argentina that is purchasing Akamai Services from Akamai Technologies Argentina S.R.L.**, (hereinafter, "the **data exporter**"), and **Akamai Technologies, Inc.**, with its place of business at 145 Broadway, Cambridge, MA 02142 USA ("hereinafter, the **data importer**"), collectively "the parties", pursuant to the terms and conditions detailed below.

Section 1. Definitions

For the purposes of this agreement, the following terms and expressions shall mean:

a) "Personal data", "sensitive information", "treatment", "responsible" and "data owner" shall have the same meanings as those established in Argentine Law 25326 of Personal Data Protection.

b) "Authority" or "regulation authority" shall mean the ARGENTINE BUREAU FOR PERSONAL DATA PROTECTION.

c) "Exporter" shall mean the person responsible for the treatment, who transfers personal data.

d) "Importer" shall mean the person responsible for the treatment residing outside the Argentine jurisdiction who receives the personal data from the data exporter for treatment pursuant to the terms hereof.

Section 2. Specific Characteristics and Treatment Purpose

The purpose and other specific details of the transfer, such as, for example, the characteristics of the personal data transferred, the manner in which the data owner's or regulation authority's requests shall be dealt with, the intended assignments or transfers to third parties, and the jurisdiction where data shall be located, are set forth in Schedule A, which forms part of this agreement. The parties may, in the future, execute additional schedules to incorporate details and characteristics of transfers subsequently carried out within the scope of this agreement.

Section 3. Data Exporter Obligations

The data exporter agrees and warrants:

a) That personal data collection, treatment and transfer has been and shall be carried out in accordance with Law 25326, and represents that it has fulfilled its duty to inform the data owners that their personal information might be transferred to a third country with lower levels of data protection than the ARGENTINE REPUBLIC.

b) That it shall provide the importer with a copy of the laws in force in Argentina that apply to the intended data treatment.

c) In the case of any exercise by the data owner of the rights conferred to him/her by Law 25326 regarding the treatment of his/her personal data as provided herein, especially of the rights to access, rectify and delete data, and other rights contained in Chapter III, sections 13 to 20, of Law 25326, that the data exporter shall address this within the legal terms and providing the means for such ends, either such request is in connection with data in the exporter's power or the exporter's agreed duty, as set forth in Schedule A. The data exporter shall answer, within the terms provided by Law 25326, the questions of the data owners and the authorities regarding personal data treatment by the importer, unless the parties have agreed that the importer should be the one to answer these questions. Even if that were the case, the exporter shall have to answer, as far as possible and based on the information that may be available to it, if the importer fails to answer.

d) That it shall make available for the data owners, as third-party beneficiaries under Section 5, upon request, a copy of such sections as may be related to the treatment of their personal data, rights and guaranties.

e) That it has made reasonable efforts to ensure that the data importer has the ability to fulfill the obligations agreed herein. For such ends, the exporter may request that the importer maintains liability insurance coverage for potential damages derived from the intended treatment, as specified in Schedule A.

Section 4. Data Importer Obligations

The data importer agrees and warrants:

a) That it shall implement the safety and confidentiality measures that may be necessary and effective to prevent data forgery, loss, unauthorized treatment or consultation, and to allow the identification of deviations, intentional or not, whether risks are derived from human acts or from the technical means used, ensuring that such measures are not inferior to those provided by the applicable rules and regulations, so as to secure the appropriate level of safety against risks involved in the treatment and nature of the data to be protected.

b) That it shall implement procedures to secure that the transferred data shall be accessed by authorized personnel only, establishing levels of access and passwords, and that said personnel shall keep said data confidential and safe, for which end specific agreements shall be entered into.

c) That it has checked that local laws do not prevent the fulfillment of the obligations, warranties and provisions provided for in this agreement in connection to the treatment of personal data and its owners, and that it shall immediately inform the data exporter should it become aware of the existence of any such law.

d) That it shall treat personal data with the aims described in Schedule A.

e) That it shall provide the data exporter with the details of a person (contact) inside its organization authorized to answer questions regarding the treatment of personal data, and that it shall cooperate in good faith with the data exporter, the data owner and the authority in connection with said questions within the legal terms. In case the data exporter has ceased to legally exist, or should the parties have so agreed, the data importer shall undertake the duties regarding compliance with the provisions of section 3, paragraph b).

f) That it shall grant access, upon request by the data exporter or the authority, to its data treatment facilities, its files and any documentation necessary for treatment, for reviewing, auditing or certification purposes. Such tasks shall be carried out, with reasonable prior notice and during regular working hours, by an impartial and independent inspector or auditor appointed by the exporter or the authority, in order to determine whether the warranties and covenants contained herein are being complied with.

g) That it shall treat personal data pursuant to Law 25326 of personal data protection.

h) That it shall give immediate notice to the data exporter about: i) any legally binding request for the assignment of personal data filed by a law enforcement authority, unless this is forbidden by the applicable law (as far as it is not in excess of what is necessary in a democratic society in accordance with the rules stipulated in item 2 of the following paragraph; ii) any accidental or unauthorized access; iii) any unanswered request received directly from the data owners, unless authorized.

i) That it shall not assign or transfer any personal data to third parties, except: 1) as specifically provided in Schedule A hereto or as necessary for its fulfillment, ensuring in both cases that the addressee abides by same terms as the importer herein, and in all cases with the exporter's prior knowledge and consent; or 2) if the assignment is required by law or by the competent authority, as far as it is not in excess of what is necessary in a democratic society, for example, when it constitutes a necessary measure to safeguard the security of the State, for defense, for public safety, for the prevention, investigation, detection and punishment of criminal or administrative offenses, or for the protection of the data owner or of other people's rights and freedoms.

Upon receiving the request mentioned above as item 2), the importer shall immediately: a) ensure that the requesting authority offers sufficient warranties regarding the fulfillment of the provisions established in Law 25326, Section 4, and of data owners' rights to access, rectify and delete data, and other rights contained in Chapter III, sections 13 to 20, of Law 25326, except in the following cases and conditions (pursuant to section 17 of Law 25326): i) those provided by law or through a decision grounded on the protection of the defense of the Nation, public order and safety, or the protection of the rights and interests of third parties; ii) through a grounded decision, notified to the affected party, when such request could obstruct court or administrative pending proceedings in connection with an investigation regarding the performance of obligations subject to state control and relating to the public order, such as: those relating to taxes, social security, the development of health and environment control functions, criminal offense

investigation, and the assessment of administrative offenses; notwithstanding the foregoing, data access shall be granted in the event the affected party needs to exercise his/her right of defense; and b) should the authority fail to provide or offer the warranties mentioned in item a) above, Argentine law shall prevail, for which reason the importer shall suspend treatment in that country, restoring data to the exporter according to the instructions given by it, and with the exporter giving notice to the regulation authority.

j) That it shall take care of such requests as it may receive from the data owner (or from the exporter, acting upon its request) regarding the rights conferred by Law 25326 regarding the treatment of his/her personal data as provided herein –as third-party beneficiary–, especially his/her rights to access, rectify and delete data, and other rights contained in Chapter III, sections 13 to 20, of Law 25326, within the legal terms and providing the means for such ends. It shall answer, within the terms established by Law 25326, questions from data owners and from the authority –also as third-party beneficiary– relating to personal data treatment carried out by the data importer, irrespective of the parties having agreed otherwise as regards who would answer these questions.

k) That it shall destroy, certifying that act, and/or restore to the exporter, as it may be agreed in the specific conditions set forth in Schedule A, all transferred personal data in the following events: 1) termination of this agreement; 2) inability to comply with the provisions of Law 25326; 3) the purpose for which data were transmitted ceased to exist. If, at such time, national legislation or local regulations applicable to the importer do not allow it to return or destroy said data in whole or in part, the importer agrees to inform the stipulated legal term and to keep said data confidential, and not to subject said data to treatment again. In the event of said maintenance period being contrary to the applicable principles of personal data protection, transfer shall not be repeated and the agreement shall be terminated, it constituting a cause of default; and if such condition were to take place during the performance hereof, this agreement shall be terminated, returning the data to the exporter according to the instructions given by it.

l) That it shall record the fulfillment of the obligations undertaken in this Section, which report shall be available upon the request of the exporter or the authority.

Section 5. Liability and Third-Party Beneficiaries

a) Each of the parties shall be liable to data owners for damages caused by said parties as a result of having affected any rights recognized by this agreement pursuant to the terms of Law 25326, its regulations and Argentine substantive law.

b) Data owners may, as third-party beneficiaries, demand that the importer complies with the provisions of Law 25326 in connection with the treatment of their personal data, pursuant to the obligations and duties undertaken by the parties herein, particularly as regards the rights to access, rectify and delete data, and other rights contained in Chapter III, sections 13 to 20, of Law 25326; to that end, they submit to the Argentine jurisdiction, both for court and administrative proceedings. In cases where default by the data importer is claimed, the data owner may demand that the exporter takes the appropriate steps to cease such default.

c) The importer agrees to the regulation authority exercising its powers as regards the data treatment undertaken by it, within the limits and with the powers provided by Law 25326, accepting such authority's powers of control and punishment, naming it -to such end and to the extent applicable- a third-party beneficiary. Auditing duties may be carried out both by regulation authority personnel and by qualified third parties appointed by said authority for such ends, or by local authorities with similar powers in collaboration with the authority.

The data importer shall inform the data exporter without delay should standing laws applicable to it or to any nominee forbid the auditing of the importer or the nominees.

d) In case the importer revokes, or fails, upon demand by the exporter, within a fixed term of FIVE (5) business days, to comply with the rights and powers granted to third-party beneficiaries pursuant to this section, that event shall constitute grounds for the automatic termination of this agreement.

e) The parties do not object to the representation of the data owners by an association or other entities stipulated in Argentine law.

Section 6. Applicable Law and Jurisdiction

This agreement shall be governed by the laws of the ARGENTINE REPUBLIC, particularly by Law 25326, its regulations and the provisions of the ARGENTINE BUREAU FOR PERSONAL DATA PROTECTION, and any controversies regarding personal data protection shall be heard by the legal or administrative courts of the ARGENTINE REPUBLIC.

Section 7. Conflict Resolution with Data Owners or the Authority

a) In the event of conflict or claim filed against one or both parties by a data owner or by the authority in connection with personal data treatment, one party shall inform the other of this circumstance and they shall both cooperate with the aim of reaching a solution as soon as possible and within the terms stipulated by Law 25326, taking an active part in any compulsory proceeding.

b) The parties agree to appear in any arbitration proceeding that may have been filed by a data owner or by the authority. If the parties choose to participate in the non-binding proceeding, they may do so remotely (for example, by telephone or through other electronic means).

c) Each of the parties undertakes to abide by any final and non-appealable decision reached by the competent courts or the authority.

Section 8. Termination

a) In the event of breach by the data importer of its obligations pursuant to the provisions hereof, the data exporter shall temporarily suspend personal data transfer to the importer until the default is remedied within the term fixed according to the seriousness of the breach, giving notice of the situation to the regulation authority.

b) The agreement shall be deemed terminated, and shall be thus declared by the exporter after the regulation authority's intervention, if: i) the transfer of personal data to the data importer has been temporally suspended by the data exporter for a period exceeding THIRTY (30) calendar days in accordance with the provisions of paragraph a); ii) performance by the data importer of this agreement and the applicable law are contrary to the legal or regulatory provisions in the import country; iii) the data importer substantially or persistently breaches any warranty or covenant provided herein; iv) a final and non-appealable decision by an Argentine court or by the ARGENTINE BUREAU FOR PERSONAL DATA PROTECTION stipulates that the data importer or exporter has breached this agreement; or v) the data exporter, notwithstanding any exercise of other rights that may be available to it against the data importer, shall be entitled to terminate this agreement when: there has been a petition for the judicial receivership or liquidation of the data importer, whether individually or as a business, and said petition has not been dismissed within the term provided for such ends, pursuant to the applicable law; an order for liquidation is issued; a receiver is appointed for any part of its assets; a bankruptcy trustee is appointed; the data importer has filed a voluntary petition for bankruptcy (*concurso de acreedores*); or the data importer is in any similar situation in any jurisdiction. In the cases mentioned in paragraphs i), ii), or iv), the data importer may also proceed to terminate the agreement without need of the regulation authority's intervention.

c) The parties agree that termination of this agreement for any reason whatsoever shall not exonerate them from the performance of the obligations and conditions regarding the treatment of transferred personal data.

Section 9. Amendments

The parties agree not to amend this agreement in any way that may imply a decrease in the level of protection and guaranties granted to the data owner and the regulation authority.

In witness whereof, this agreement is executed in two equal counterparts.

Date: 22-9-2020

By the DATA IMPORTER:

Date: _____

By the DATA EXPORTER

SCHEDULE A

DESCRIPTION OF THE TRANSFER

Data subjects
The personal data transferred concern the following categories of data subjects:
The internet end users accessing the web sites and/or web-services of the data exporter's customers and for Enterprise Security Personal Data (as defined below), the employees of the data exporter's customers.

Purposes of the transfer(s)
The transfer is made for the following purposes:
The development and usage of the Akamai cyberthreat intelligence, improving the Akamai serivces, assessing and managing the state of the traffic on the Akamai platform.

Categories of data

The personal data transferred concern the following categories of data:

a) End User Personal Data

The data importer processes Personal Data included within the web content of the data exporter's customers ("End User Personal Data") when providing the Services to the data exporter's customers. Upon a customer's choice, End User Personal Data may include data such as:

a. Login credentials;

b. Subscriber name and contact information;

c. Financial or other transaction information;

d. Other Personal Data relating to the individual data subject as set by Customer.

b) Logged Personal Data

The data importer processes Personal Data that is included in log files when performing the Services for the data exporter's customer (Logged Personal Data"). Logged Personal Data is Personal Data logged by Akamai servers, relating to the access to customer content over the Akamai platform by Customer's end users, as well as logged personal data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's session with the customer's web property. Logged Personal Data include such data as:

a. End user IP addresses;

b. URLs of sites visited with time stamps (with an associated IP address);

c. Geographic location based upon IP address and location of Akamai server;

d. Telemetry data (e.g., mouse clicks, movement rates, and related browser data).

c) Site Personal Data

The data importer processes Personal Data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's session with the Customer's web property ("Site Personal Data"). The Site Personal Data consists of user telemetry data (e.g., mouse clicks, movement rates, and user agent and related browser data) designed to measure website performance.

d) Enterprise Security Personal Data

The data importer processes Personal Data on behalf of Customers of Akamai Enterprise Security Services that are provided by the data exporter's customer or collected during the provision of services in order to protect users of the customer's enterprise network and the network itself from Internet security and policy abuse risks ("Enterprise Security Personal Data"). The Enterprise Security Personal Data includes such data as:

a. Login and user authentication data;

b. Contents of communications, including attachments

c. Browser and device information, including location information

d. URLs visited

e) Special categories of data

The data exporter's customer as the Data Controller decides the categories of data that is included in the End User Personal Data. Where Customer chooses to include special categories of data in the Customer Content, the data importer will process this data as End User Personal Data, as instructed by the customer.

f) Categories of data processed by particular Akamai Services

Akamai maintains a list of service categories that provide further information regarding the processing of Personal Data conducted in providing Services in each category. This list is available at www.akamai.com/compliance/privacy/.

Recipients

The personal data transferred may be received only by the following recipients or categories of recipients:

The employees of the data importer, the employees of the data exporter and the customer's employees.

Additional useful information (storage limits and other relevant information)

The retention period of End User Personal Data is determined by the data exporter's customers. The retention period for Logged Personal Data and Enterprise Security Personal Data is 90 days. The retention period for Site Personal Data is 18 months. Where personal data is retained by the data importer, such data is retained on systems deployed in the United States.

Contact points for data protection enquiries and data access requests

Contact point for the data importer:
Jim Casey, Akamai Technologies Chief Data Protection Officer,
privacy@akamai.com

Contact point for the data exporter:
Dr. Anna Schmits, Akamai Technologies EMEA DPO,
privacy@akamai.com

The process to submit data access requests and to file a complaint is described in the data importer's privacy statement, available at https://www.akamai.com/us/en/multimedia/documents/akamai/akamai-privacy-statement-july-2018.pdf.
