DATA TRANSFERS

BRAZILIAN STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of applicable dispositions of the Brazilian Law No. 13709/18 ("**LGPD**"), for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Partner
Address: As stated in the agreement between Partner and LiveRamp
(the "**data exporter"**)
And
Name of the data importing organisation: LiveRamp France
Address: 25-29 rue Anatole France, 92300 Levallois-Perret, France

(the "**data importer"**)

each a 'party'; together 'the parties',
HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in the LGPD;
(b) 'the data exporter' means the controller who transfers the personal data;
(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of the LGPD;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in Brazil;
(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter,

in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities) and does not violate the relevant legal provisions;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of the LGPD;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

  (ii) any accidental or unauthorised access; and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject: (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; (b) to refer the dispute to the competent courts.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the applicable law as agreed by the Parties in their agreement.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses ([1]). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the applicable law as agreed by the Parties in their agreement.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The supervisory authority may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix**.**

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
Partner

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
LiveRamp Inc.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
Users of Partner's websites

Categories of data
The personal data transferred concern the following categories of data (please specify):
Presence of RampID Envelope, bidder name, bid ID, auction ID, user browser, user platform/OS, timestamp(s), domain, Partner's placement ID, currency, cost per mille, and net revenue

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
None.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
Provision by LiveRamp to Partner of analytics reports related to their use of the Authenticated Traffic Solution by using Partner Analytics Data.

Appendix 2
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. **General.** LiveRamp shall use industry-standard security measures designed to protect against unauthorized access, loss and misuse of hashed or encrypted IDs, including encryption of stored information behind a secured server network and organizational, contractual, technological and managerial safeguards as more thoroughly described herein. LiveRamp security measures may be subject to change at LiveRamp's sole discretion, however any such changes shall not diminish or reduce the requirements provided herein. All capitalized terms that are not expressly defined herein shall have the meanings given to them in the Agreement.
2. **Shared Processing Environment.** To provide its Products and Services LiveRamp may perform the Services from a facility that is owned by a third party, a portion of which is available for use by LiveRamp or its Affiliates through a co-location arrangement, or a similar environment that is managed by LiveRamp Personnel. Any such facility, location, or environment must meet, in all material respects, the applicable requirements established herein.
3. **Safeguards.** LiveRamp shall maintain reasonable administrative, technical and physical controls designed to ensure the privacy, security, and confidentiality of Client Data ("Safeguards"), that comply with this Attachment, applicable industry standards, and Laws, including:
    a. **Physical Access**. LiveRamp shall maintain physical access controls designed to secure relevant facilities, infrastructure, data centers, hard copy files, servers, backup systems, and equipment (including mobile devices) used to access Client Data, including controls to prevent, detect, and respond to attacks, intrusions, or other system failures. LiveRamp shall log physical access, conduct semi-annual reviews, and require visitors to sign in and out of facilities housing systems that process, store, or transmit Confidential Information.
    b. **User Authentication.** LiveRamp shall maintain user authentication and access controls within operating systems, applications, equipment, and media.
    c. **Personnel Security.** LiveRamp shall maintain personnel security policies and practices restricting access to Client Data, including written confidentiality agreements and background checks consistent with applicable law for all personnel with access to Client Data or who maintain, implement, or administer LiveRamp's information security program and Safeguards.
    d. **Logging and Monitoring.** LiveRamp will log and monitor the details of access to Confidential Information on networks, systems, and devices operated by LiveRamp. LiveRamp logging and monitoring systems must meet applicable industry standards.
    e. **Malware Controls**. LiveRamp will maintain reasonable and up-to-date controls to protect networks, systems, and devices that access Client Data from malware and unauthorized software.
    f. **Security Patches**. LiveRamp will maintain controls and processes designed to ensure that networks, systems, and devices (including operating systems and applications) that access Client Data are up-to-date, including application of security updates and patches to systems and applications that process Client Data at least according to the manufacturers' best practice recommendations or guidelines and LiveRamp must test patches, service packs, and hot fixes before installing them, according to LiveRamp's operational change management program.
    g. **User Account Management.** LiveRamp shall implement reasonable user account management procedures to securely create, amend, and delete user accounts on LiveRamp networks, systems, and devices, including monitoring redundant accounts and ensuring that information owners properly authorize user account requests. LiveRamp shall continually manage its user accounts. User account management shall include unique user IDs for access, a review of user access rights every 6 months at most, a review of privileged user access rights quarterly, and allow limited and controlled access to LiveRamps's internal network.
    h. **Password Requirements.** LiveRamp shall maintain a password policy for systems and applications that process Confidential Information that, at a minimum, requires passwords **to**: (i) be a minimum of ten (10) characters in length; (ii) contain a mix of upper and lower case letters and at least one number and one special character; (iii) not be the username; (iv) expire at least every 90 days; (v) not be the same as any previous 6 passwords; (vi) be changed at the first logon after initial password; (vii) be encrypted at rest and in transit; (viii) be masked when entered into a system or application; (ix) lock accounts after 5 invalid login attempts; (x) not be a PIN or secret question that is any less secure than the primary authentication password or mechanism; and (xi) have a minimum password age.
4. **Encryption Requirements.** Using a reasonable encryption standard, LiveRamp will encrypt all Client Data that is (a) stored on portable devices or portable electronic media; (b) stored or maintained outside of LiveRamp's facilities, excluding hard copy documents; or (c) transferred across any network other than an internal company network owned and managed by LiveRamp.
5. **Access Controls.** LiveRamp shall: (a) maintain reasonable controls to ensure that only individuals who have a legitimate need to access Client Data under the Agreement will have such Access; (b) promptly terminate an individual's Access to Client Data when such access is no longer required for performance under the Agreement; and (c) log the appropriate details of access to Client Data on it's systems and equipment.
6. **Training and Supervision.** LiveRamp shall provide ongoing privacy and information protection training and supervise it's personnel who access Client Data.

7. **Assessments; Audits; Corrections.**
    a. **Client Audits and Assessments.** Upon Client's written request, to confirm compliance with this Attachment, LiveRamp will once annually, promptly and accurately complete Client's written information privacy and security questionnaire regarding LiveRamp's information privacy and security practices in relation to all Client Data that LiveRamp receives in order to provide the Services. Furthermore, and no more than once annually, upon written request which must be given at least ten (10) business days in advance, Client or its designated representative may assess and audit LiveRamp's compliance with this Attachment, LiveRamp's responses to Client's information privacy and security questionnaire, or LiveRamp's compliance with privacy Laws to determine if it is adequate to protect Client Information and may, request improvements of the security controls to prevent malicious or inappropriate access to source code, data, graphics or audio/visual material used to perform services for Client. Notwithstanding the foregoing, or anything to the contrary in the Agreement, LiveRamp shall have no obligation to provide Client access to its systems, or provide Client certain information from its shared processing environments, including, but not limited to, records of internal vulnerability scans and penetration tests, systems logs, detailed network diagrams, and application code.
    b. **LiveRamp- Audits and Assessments.** LiveRamp will continuously monitor risk to Client Data to ensure that the Safeguards are properly designed and maintained to prevent unauthorized access to Client Data and will periodically (but no less than once per year) assess and document the effectiveness of its Safeguards across its networks, systems, and devices (including infrastructure, applications, and services) used to access Client Data and update its Safeguards as needed. In addition to any internal audits, LiveRamp shall conduct an annual privacy and security audit of its Safeguards covering all relevant networks, systems, devices, and media used to access Client Data using a recognized third party audit firm and a reasonable audit standard. Upon Client's written request, LiveRamp shall provide Client a SOC 2 Report as may be applicable, as a Statement on Standards for Attestation Engagements (SSAE) No. 18 audit, ISAE 3402, or equivalent audit completed by such firm.
    c. **Vulnerability Testing.** LiveRamp shall periodically (but at least once per quarter) perform manual and automated vulnerability testing (including penetration testing based on recognized industry best practices) on all LiveRamp internet-facing networks, systems, software and devices used to access Client Data. Upon written request from Client, LiveRamp shall provide evidence of such testing, which shall include a statement of opinion for vulnerability and penetration testing completed on LiveRamp internet facing systems. Client shall have no right to perform vulnerability or penetration testing on LiveRamp networks or systems.
    d. **LiveRamp Response to Audits.** Upon Client's written request, the Parties may meet promptly upon the completion of any audit conducted pursuant to this Attachment and/or the issuance of an interim or final report following such an audit. The Parties shall review and escalate such audit findings as and to the extent necessary. LiveRamp shall respond to each exit interview and/or audit report in writing within thirty (30) days, unless a shorter response time is specified in such report, and agreed upon by LiveRamp. The Parties shall develop and agree, upon an action plan to promptly address and resolve any deficiencies, concerns and/or recommendations identified in such exit interview or audit report. LiveRamp, shall then undertake remedial action in accordance with such action plan, at the dates specified in such action plan to the extent necessary to comply with LiveRamp's obligations under this Attachment.
8. **Security Breach Response.** LiveRamp shall maintain policies and procedures for responding to Security Breaches, including without limitation, assigning and training a Security Coordinator, training employees, subcontractors, suppliers, vendors, agents and representatives having access to Client Data on the policies and procedures to recognize Security Breaches and escalate and notify the Security Coordinator of any Security Breach. "Security Breach" shall mean any actual or reasonably suspected: (1) unauthorized access to or theft of Client Data; (2) unauthorized use of Client Data by a person with authorized access to the information for purposes of actual or reasonably suspected theft, fraud or identity theft; (3) unauthorized disclosure or alteration of Client Data ; or (4) loss of Client Data, including without limitation, any of the foregoing described in (1) – (3) caused by or resulting from a failure, lack of or inadequacy of security, physical intrusion of facilities, theft or loss of documents, laptops or storage media, or employee or contractor malfeasance. If LiveRamp has a Security Breach it shall handle such breach in accordance with its Security Incident Response Guide and:
    a. Notify Client within 72 hours after the discovery of the Security Breach;
    b. Use commercially reasonable efforts and take all necessary actions to prevent, contain, and mitigate the impact of the Security Breach;
    c. Promptly and in no event more than 7 business days after the Security Breach provide a written status report;
    d. Collect and preserve all evidence concerning the discovery, cause, vulnerability, exploit, remedial actions and impact related to the Security Breach, which shall be forensically admissible in legal proceedings;
    e. Document incident response and remedial actions taken in detail, which shall be forensically admissible in legal proceedings; and

Allow Client to contract with a qualified third party, upon LiveRamp approval to assist in the investigation and review relevant documentation onsite under the direction of LiveRamp corporate security. For the avoidance of doubt, "internal use only" documentation as well as systems logs from shared processing environments shall not be shared with Client its designated third party.