/LiveRamp

225 Bush St. Floor 17, San Francisco, CA 94104

# RampID Data Protection Attestation

Based on your service agreement with LiveRamp, your company will receive a file containing RampIDs that will facilitate analytics across datasets (e.g., impression data, segment data, transaction data). This attestation form is intended to ensure that these **RampIDs will not be re-identified and you will implement the controls found here.** If you need assistance with the requirements below, contact your account representative.

I certify, as an authorized representative of my company, that we will adhere to the following requirements for the RampIDs received from LiveRamp will not be:

- used to re-identify the associated individual
- stored or merged with PII, re-identified, or reverse engineered
- used to re-identify cross-context browsing information
- shared with companies or entities restricted by law, including entities sanctioned by the US government

I agree to notify LiveRamp of any changes to my company's ability to comply with the requirements below.

**RampID Environment Requirements**

Where your company has access to (i) raw PII, and (ii) Cross-Context Browsing Information, and/or (iii) RampIDs, Company shall establish technical and administrative controls including the isolation of systems to prevent Cross-Context Browsing Information and/or the RampID from being linked to raw PII via a RampID environment as described herein. This requirement is to prevent unauthorized access to the linkage and prevent use of both data elements together.

Your company must follow the following specific requirements:

- PII must be stored in a secure environment that is separate from any environment(s) that contains Cross-Context Browsing Information and/or RampIDs.
    - An example of logically-separated environments is where data is separated using access controls, though all data is stored on the same server.
    - Another example of logically-separated environments is where PII and RampID-associated data are stored in separate locations (separate projects is enough) with controls preventing commingling of data.
- PII must be transformed using a one-way hashing method before being stored with Cross-Context Browsing Information and/or RampIDs.
    - This process should not at any time produce a mapping table between PII and online identifiers.
    - Users with access to the RampID environment should not have access to the hashing algorithm/salt/encryption key used to transform the PII.
    - It is best practice to enable a third group of users to perform or monitor the data transformation.
    - Where possible, data transformations should be logged for auditing.
- No movement of data should occur from the RampID environment to an environment containing PII.
- User Controls:
    - No user should have access to both the RampID and PII environments. If this is not possible, then:
        - The user should use separate logins for each environment.
        - PII should be encrypted and the user should not have access to the decryption key.
    - User access to RampID and PII environments and activity within those environments should be logged.
    - No user should have the capability to modify the access and activity logs.
    - Users having access to the RampID environment have been trained on data security and privacy best practices.

"*Cross-Context Browsing Information*" means information collected about end users' visits to websites, apps, or other online properties that are not owned by the same company; Cross Context Browsing Information does not include any data the Participant collects from end users in a first-party context.

*"Personally identifying information" or "PII"* is information that directly identifies an individual, including name, email address, or phone number or an identifier linked directly to PII such as a customer loyalty number. LiveRamp supports PII such as email address and phone number, and translates the PII to a RampID that can be used for the purpose of collaboration and targeted advertising but cannot by itself be traced back to the original value.