LAUNCHMETRICS

Data Processing Agreement

This Personal Data Processing Agreement ("**Processing Agreement**") between Customer and Service Provider, sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by Service Provider ("**we**", "**our**" or "**us**") to Customer pursuant to the Launchmetrics Service Provider Agreement (the"**Agreement**").

For the avoidance of doubt, any capitalized terms not defined in this Processing Agreement shall have the meanings set forth for such terms elsewhere in the Agreement.

In consideration of the mutual covenants and agreements in this Processing Agreement and the Service Provider Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Service Provider agree as follows:

I. GENERAL

1.1. **Term and Entry into force.** For the avoidance of doubt, this Processing Agreement shall continue in full force and effect until the date of termination of the Original Agreement and is applicable from its signature, however the commitments listed below do not come into effect until May 25, 2018.

II. DEFINITIONS

2.1. "Applicable Data Protection Laws" 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 Service Provider in the United States and in the EU including the laws of any member of the EU and the General Data Protection Regulation *(EU) 2016/679* ("**GDPR**") and any other national implementing laws, regulations and secondary legislation, as amended or updated from time to time in Spain and their successor legislations.

2.2. "Data Controller" has the meaning defined in the GDPR.

2.3. "Data Processor" has the meaning defined in the GDPR.

2.4. "EEA"means the European Economic Area.

2.5. "Personal Data" means any information relating to an identified or identifiable natural person such as name, last name, email address, postal address, telephone number, date of birth, Social Security number (or its equivalent), driver's license number, account number, credit or debit card number, location data, identification number, health or medical information, any other unique identifier or one or more factors specific to an individual's physical, physiological, genetic, mental, economic, cultural or social identity or that is defined as "Personal Information," "Personally Identifiable Information," "Sensitive Personal Data," "Personal Data," "Special Categories of Personal Data", or any similar designation by Applicable Data Protection Laws, in any form and any media, that Service Provider receives, accesses, collects, processes, generates, compiles or creates in connection with this Agreement.

2.6. "Process" or "Processing" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as creation, collection, procuration, obtaining, accession, recording, organisation, storage, adaption or alteration, retrieval, consultation, dissemination or otherwise making available, use, disclosure by transmission, restriction, erasure or destruction.

2.7. "Technical and Organisational Security Measures" means those measures aimed at protecting personal data against unlawful destruction or accidental destruction or loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing.

III. DATA PROTECTION

3.1. **Compliance with Laws**. Both parties will comply with all requirements of the Applicable Data Protection Laws.

3.2. **Role of the Parties**. This Processing Agreement applies when Customer Personal Data is processed by Service Provider. Customer acts as Controller with respect to Customer Personal Data and Service Provider acts as Processor.

3.3. **Processing Instructions**. Service Provider shall Process Personal Data when performing its obligations under this Agreement only on the written instructions of Customer and Service Provider agrees to act in accordance with the instructions of Customer. Service Provider shall inform Customer in writing as soon as is commercially and reasonably practicable if it cannot comply with Customer's instructions. If Service Provider cannot comply with Customer's instructions, Customer can suspend the transfer or disclosure to or access by Service Provider of Personal Data and terminate any further Processing of Personal Data by Service Provider, if doing so is necessary to comply with Applicable Data Protection Laws.

3.4. **Description of the Personal Data Processing by Service Provider.** A list regarding the scope and duration of processing, categories of Data Subjects, and types of Personal Data processed, is set out in the applicable DPA Exhibit A.

3.5. **Inquiries on Processing.** Service Provider shall deal promptly and appropriately with any inquiries from Customer relating to the Processing of Personal Data Subject to this DPA or the Original Agreement.

3.6. **Launchmetrics Personnel.**

3.6.1 **Confidentiality Obligations.** Service Provider warrants that except and solely as permitted in the applicable Section in the Original Agreement, Service Provider and its employees, agents, consultants and contractors shall hold in strict confidence (i) the existence and terms of this DPA, the Agreement and any related agreement; (ii) any and all Personal Data (whether in individual or aggregate form and regardless of the media in which it is contained) that may be disclosed at any time to Service Provider or its employees, agents, consultants or contractors by Customer, Customer's Affiliates or their respective employees, agents, consultants or contractors in anticipation of, in connection with or incidental to the performance of services for or on behalf of Customer or Customer's Affiliates; (iii) any and all Personal Data (whether in individual or aggregate form and regardless of the media in which it is contained) that may be Processed at any time by Service Provider or its employees, agents, consultants or contractors in connection with or incidental to the performance of services for or on behalf of Customer or Customer's Affiliates; and (iv) any information derived from the information described in (ii) and (iii) above; ((ii), (iii) and (iv) designate collectively: Personal Data; provided, however, that the Parties agree that any materials or information used in or resulting from any activities that Service Provider is allowed to engage in pursuant to the applicable Section in the Original Agreement shall be deemed to not constitute "Personal Data" even if such information or materials used in such activities might constitute or include "Personal Data" in other contexts).

3.6.2 **Limitation of Access.** Service Provider shall ensure that Service Provider's access to the Personal Data is limited to those personnel who require such access to perform the Original Agreement and are obliged to keep the Personal Data confidential.

3.6.3 **Supervision and Awareness.** Service Provider shall exercise the necessary and appropriate supervision over its relevant employees, contractors, consultants, agents, vendors and partners to maintain appropriate privacy, confidentiality and security of Personal Data. Service Provider shall provide training, as appropriate, regarding the privacy, confidentiality and information security requirements set forth in this DPA to employees, contractors, consultants, agents, vendors and partners with access to Personal Data.

3.6.4 **Data Protection Officer.** Members of the Service Provider Group will appoint a Data Protection Officer where such appointment is required by Applicable Data Protection Laws and Regulations. The appointed person may be reached at dpo@launchmetrics.com.

3.7. **Return and Deletion of Customer Data.** Promptly upon the expiration or earlier termination of the Agreement, or such earlier time as Customer requests, Service Provider shall, at the choice of Customer, securely return to Customer or its designee, or, securely destroy or render unreadable or undecipherable if return is not reasonably feasible or desirable to Customer (which decision shall be based solely on Customer's written statement), each and every original and copy in every media of all Personal Data in Service Provider's possession, custody or control. Service Provider shall comply with all directions provided by Customer with respect to the return or disposal of all Personal Data unless otherwise required by Applicable Data Protection Laws.

3.8. **Transfer Mechanisms.** Service Provider shall not transfer any Personal Data outside the EEA unless the prior written consent of Customer has been obtained and the following conditions are met:

- Customer or Service Provider has provided appropriate safeguards (such as binding corporate rules, the Model Clauses, the Privacy Shield, etc.) in relation to the transfer as per Article 46 GDPR;
- The Data Subject has enforceable rights and effective legal remedies;
- Service Provider complies with its obligations under Applicable Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and;
- Service Provider complies with reasonable instructions notified to it in advance by Customer with respect to the Processing of Personal Data.

IV. SUBCONTRACTORS

4.1. **Appointment of Subcontractors.** Customer consents to Service Provider subcontracting its obligations under this Agreement to affiliated companies or third-party processors to perform and fulfil the Service Provider's commitments and obligations under this Original Agreement. Service Provider confirms that it has entered or (as the case may be) will enter with (each of) the third-party processor(s) into a written agreement incorporating terms which are substantially similar to those set out in this DPA as between Customer and Service Provider and, such third-party processor has given sufficient guarantees that they will implement measures to ensure that processing the Personal Data it carries out will meet the requirements of the GDPR and protect the rights of Data Subjects.

4.2. **Subcontractors List.** When applicable, Service Provider shall maintain an up-to-date list of Subcontractors, specifying (i) their name and details, as well as (ii) the nature of the tasks entrusted to them, and (iii) the location of the Processing.

4.3. **New Subcontractors.** Service Provider shall give Customer prior written notice of the appointment of any new Subcontractor, including full details of the Processing to be undertaken by the Subcontractor.

4.4. **Objection Rights.** To avoid doubt, it shall be reasonable for Customer to withhold or deny such consent if Customer has reasonable doubts that a Subcontractor is able to perform and fulfil the Service Provider's commitments and obligations under this DPA. The objection must be based on reasonable grounds (e.g. if Customer proves that significant risks for the protection of its Personal Data exist at the subcontractor).

4.5. **Subcontractors in a third country.** Customer hereby authorizes Service Provider, to agree in the name and on behalf of Customer with a subcontractor which processes or uses Personal Data of Customer outside the EEA, to enter into EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries dated 5 February 2010 ("**Standard Contractual Clause**"). This applies accordingly from the date of this authorization with respect to Standard Contractual Clause already concluded by Service Provider with such Subcontractors.

4.6. **Liability.** Service Provider shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this section.

V. RIGHTS OF DATA SUBJECTS

5.1. **Data Subject Request.** To the extent permitted by law, Service Provider will inform Customer as soon as is commercially and reasonably practicable, in writing of any requests with respect to Personal Data received from Customer's customers, consumers, employees or others ("**Data Subject**") to exercise the following Data Subject rights: access, rectification, restriction of Processing, erasure ("**right to be forgotten**"), data portability, objection to the Processing, or to not be subject to an automated individual decision making. Service Provider shall assist Customer, at Customer's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, impact assessments and consultation with supervisory authorities or regulators, or access or rectification of Personal Data pertaining to a Data Subject.

VI. SECURITY

6.1. **Data Property.** All Personal Data shall at all times be and remain the sole property of Customer, and Service Provider shall not have or obtain any rights therein.

6.2. **Technical and Organizational Measures.** Service Provider shall take appropriate Technical and Organizational Security Measures against unauthorized or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, the Personal Data provided by Customer appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of the technological development and the cost of implementing any measures where appropriate, for example, pseudonymisation and encryption of Personal Data.

6.3. **Controls for the Protection of Customer Data.** Service Provider shall develop, maintain and implement a comprehensive written information security program that includes appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data, (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data, and (iii) protect against any Information Security Incident. Service Provider regularly monitors compliance with these measures.

6.4. **Security Incident and Personal Data Breach Management and notifications.** Service Provider will notify Customer without undue delay in writing after becoming aware of any violation of any provision of this Processing Agreement or any actual or suspected theft or unauthorized Processing, loss, use, disclosure or acquisition of, or access to, any Personal Data (hereinafter "**Customer Security Incident**") of which Service Provider becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under Applicable Data Protection Law or which Service Provider is required to notify to Customer under Applicable Data Protection Law. Service Provider shall provide commercially reasonable cooperation and assistance in identifying the cause of such Customer Security Incident and take commercially reasonable steps to remediate the cause to the extent the remediation is within Service Provider's control. The obligations herein shall not apply to incidents that are caused by Customer, Authorized Users, any NonLaunchmetrics-related Products or Force Majeure.

6.5. **Audits.** Service Provider shall maintain complete and accurate records and information to demonstrate its compliance with its obligations under this Agreement and also for audits conducted by or on behalf of Customer. Customer may contact Service Provider in accordance with the "Notice" Section of the Original Agreement to request an on-site audit of Service Provider' procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Law. Before the commencement of any such on-site audit, Customer and Service Provider shall mutually agree in writing upon the scope, timing, and duration of the audit. Customer will restrict its audit activity to the departments and locations agreed upon in writing. A schedule of meetings and audit activities will be detailed in writing with the nominated single point of contact for the audit and the identified business areas. Customer must provide Service Provider with a notice of fifteen (15) days. Customer can perform a new audit within three years following the former scheduled audit. Customer is responsible for the cost and expenses of the audit. Customer must sign a NDA before each audit. Customer's audit team is legally bound by Service Provider's NDA which prohibits Customer from knowingly and recklessly disclose any Confidential information pertaining to the audit. Customer shall promptly notify Service Provider with information regarding any noncompliance discovered during the course of an audit, and Service Provider shall use commercially reasonable efforts to address any confirmed non-compliance.

6.6. **Judicial Access.** Subject to applicable law, Service Provider shall notify Customer as soon as is commercially and reasonably practicable in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Customer shall have the right to defend such action in lieu of and on behalf of Service Provider. Customer may, if it so chooses, seek a protective order. Service Provider shall reasonably cooperate with Customer in such defense.

VII. AMENDMENT(S) OF THE PROCESSING AGREEMENT

This Processing Agreement may be amended in the light of developments, laws and regulations, including those of the Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) and the GDPR as they exist to date and as they could be amended and, to any other rule, law, recommendation, regulation of the Spanish Data Protection Authority or any competent European Supervisory Authority.

EXHIBIT 1

Details of the Processing

The details of the Processing by the Service Provider under this Agreement are as follows:

Scope and legal basis of Processing:

Service Provider will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Agreement's Schedule detailing the subscribed Services. For further information regarding the Processing related to a particular Service, please see the online Privacy Policy (User Policy) applicable to the Service.
The legal basis of the processing is the execution of the Agreement.

Nature and Purpose of Processing:

Service Provider will only Process Personal Data to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Duration of Processing:

Service Provider will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or legally required.

Types of Personal Data Processed: Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

First and Last name

Job position

Contact information

ID Data

Social media Data

Professional life Data

Personal life Data (i.e. birthdates)

Connection Data (i.e. login)

Localisation Data

Data Controller for User Data:
The Data Controller is Augure Spain SU with registered office in Calle Orense, Número 6, Primera Planta – Local 5, 28020 Madrid, Spain
Tax code 84345602

Usage Data

Payment data

Categories of Data Subjects: Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Customer itself
- Employer or business relations of Customer
- Individuals or organizations in a relationship with Customer

Rights of the Data Subject

In your capacity as a Data Subject, you have the right to:

- access to Data;
- oppose to Processing;
- rectification, erasure, restriction of Data Processing;
- transfer (data portability);
- as well as withdraw consent or send a complaint to the Supervisory Authority

It should be noted that the right of opposition of the Data Subject for direct marketing purposes or of third parties through automated methods extends to traditional ones and that in any case the possibility remains for the Data Subject to exercise the right to oppose even partially. Therefore, the Data Subject may decide to receive only communications using traditional methods or only automated communications or none of the two types of communication.

How to exercise rights

You can exercise your rights at any time by sending a communication to one of the following e-mail addresses: supporto@launchmetrics.com or dpo@launchmetrics.com.

EXHIBIT 2

Description of the technical and organisational security measures implemented

1. Application Level.
   1.1. Regularly scheduled security audits, both internal and external
   1.2. External security audits and vulnerability scans performed by TrustWave. The results of these audits are available to Customer on request.
   1.3. Use of Secure Sockets Layer (SSL/TLS)
   1.4. Strong cryptographic standards, including advanced password hashing techniques
   1.5. Strong incident management, change control and asset management policies.
   1.6. Access to applications is restricted only to whitelisted IP addresses (if requested by Customer): customers can choose to have their data and application be accessible only from IP addresses that they specify during the setup.
   1.7. Password Authentication for all users: only Authorised Users have access to the application. In addition, there are different levels of authorisation. For example, users not authorised for administrator access cannot add or remove users.
   1.8. Support for different roles and permissions for each role. Permissions can be set at the role level or at individual users' level. Only roles or user authorised to access a protected resource can do so.
   1.9. All User activity is logged: In the event of unauthorised activity, we can review the log to investigate the events and provide the log to Customer if requested.
   1.10. Use one-time password authentication for critical systems. AWS, Gmail, Github, Lastpass applications are all secured with the second layer of OTP system where the user is required to input username and password as well as the code shown on the authenticator application.

2. Disaster Recovery.
   2.1. Full Data backups every 24 hours.
   2.2. All servers are secured and distributed behind load balancers. Service Provider is able to detect the traffic and do maintenance in the servers without affecting Customer service.
   2.3. Backups are kept locally as well as at remote location on S3.
   2.4. Thirty (30) days of data backups retained.
   2.5. In case of total loss of data centre or data, Customer can be moved to secondary data centre with most recent data backup in less than 4 hours.

3. Hosting.
   3.1. Servers are hosted in several state-of-the-art Data centres certified SSAE and ISO 27001.
   3.2. Equipment is behind multiple layers of physical security and supported by redundant power and HSRP/VRRP Internet access. The Data Centre is located at heavily protected buildings where the security personnel are on guard 24x7. Other security features include biometric fingerprint readers on door locks, strategically placed cameras and motion detection, and doors equipped with alarm system.
   3.3. Remote access to Launchmetrics network within AWS Data centre is only allowed to authorised employees over a secure VPN connection.

4. Office Network.
   4.1. The office network is protected by Cisco Firewall. Only authorised access is permitted.
   4.2. Documents are shared only among authorised employees. Documents on the office network are not public and can only be accessed by authorised employees or consultants.
   4.3. Access to the building is not granted unless the visitor is pre-authorised or a current employee allows access.

5. Updates. Service Provider is constantly improving its Services and platform. Service Provider's latest Technical and Organisational Security Measures updates are available on request. Customer may write to Service Provider using the following email address support@launchmetrics.com and asking for the following document: Launchmetrics - Security Policy and Practices.docx.

EXHIBIT 3

List of Subcontractors

Infrastructure Subprocessors – Service Data Storage

Entity Name	Entity Type	Entity Country
Amazon Web Services, Inc.	Cloud Service Provider	United States
Amazon Data Services Ireland Ltd (upon Customer request)	Cloud Service Provider	Ireland

Launchmetrics Group

Entity Name	Country
Fashion GPS, Inc. d/b/a Launchmetrics	United States
Fashion GPS Europe Ltd.	United Kingdom
Augure SA	France
Augure Spain SL	Spain
Visual Box Srl.	Italy
Launchmetrics Technologies Srl.	Romania
Style Coalition LLC.	United States
Launchmetrics Germany GmbH	Germany

Service Specific Subprocessors

- Salesforce.com, Inc. – United States – CRM
- Google LLC – United States – Customer Support
- Oracle America, Inc. – United States –Billing and Customer Support

(Complete if applicable)