LAUNCHMETRICS

Data Processing Agreement

BY AND BETWEEN

Launchmetrics Germany GmbH, a limited liability company registered in the Commercial Register of Munich Local Court under HRB 245516 having its principal offices at Leopoldstraße 8-10,12 in 80802 Munich, Germany, (the "Service Provider")

AND

the "Customer"

(the Company and the Customer, each a "Party" and, together, the "Parties")

WHEREAS

A) Service Provider provides to its clients certain services, including marketing intelligence, influencer campaign management and launch to market campaigns mainly in the fashion, luxury and beauty sector (the "Services");

B) The Parties, by means of this Data Processing Agreement (the "Processing Agreement") wish to implement the current legal framework in relation to data Processing and, in particular, the Regulation EU 2016/679 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data.

THE PARTIES AGREE AS FOLLOWS

1. Definitions.

1.1 In this Processing Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "Applicable Laws" means the European Union or Member State laws, including the EU Data Protection Laws, to which the Company or any Company Group Member is subject;

1.1.2 "Company Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Service Provider, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "EU Data Protection Laws" means including by the GDPR and laws implementing or supplementing the GDPR;

1.1.4 "GDPR" means EU General Data Protection Regulation 2016/679.

1.1.5 "Sub Processor" means sub processor expressly appointed by or on behalf of the Company to Process Personal Data;

1.1.6 "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.

1.2 The terms, "Commission", "Controller", "Processor", "Data Subject", "Member State", "Personal Data", "Processing", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Personal Data.

2.1 Compliance with Laws. Both parties will comply with all requirements of the Applicable Laws.

2.2 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 regarding Customer Personal Data.

2.3 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 Laws.

2.4 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 Exhibit A.

2.5 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 Processing Agreement or the Agreement.

3. Launchmetrics Personnel.

3.1 Confidentiality Obligations. Service Provider ensures confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. Service Provider entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. Service Provider and any person acting under its authority who has access to personal

data, shall not process that data unless on instructions from the Customer, which includes the powers granted in this contract, unless required to do so by law. 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 Processing Agreement, 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 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).

3.2 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 Agreement and are obliged to keep the Personal Data confidential.

3.3 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 Processing Agreement to employees, contractors, consultants, agents, vendors and partners with access to Personal Data.

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

4. Return and Deletion of Customer Data.

4.1 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 Laws.

4.2 Service Provider may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that

Service Provider shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

5. Sub Processors.

5.1 Customer authorizes Service Provider to appoint Sub Processors in accordance with this Section. Service Provider may continue to use those Sub Processors already engaged by Service Provider at the date of this Processing Agreement.

5.2 Sub Processing. For the purpose of this Processing Agreement, Sub Processing services is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Service Provider shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure compliance with Applicable Laws, even in the case of outsourced ancillary services.

5.3 Appointment of Sub Processors. Service Provider may commission Sub Processors only after prior explicit written or documented consent from the Customer. Outsourcing to Sub Processors or changing the existing Sub Processors is permissible when:

- Service Provider submits such an outsourcing to a Sub Processor to the Customer in writing or in text form with appropriate advance notice; and
- The Customer has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to Service Provider; and
- The Sub Processing is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

The Customer hereby authorizes Service Provider, to agree in the name and on behalf of the Customer with a Sub Processor 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 Sub Processors.

5.4 Sub Processors List. When applicable, Service Provider shall maintain an up-to-date list of Sub Processors, 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.

5.5 New Sub Processors. Service Provider shall give Customer prior written notice of the appointment of any new Sub Processor, including full details of the Processing to be undertaken by the Sub Processor.

5.6 Further outsourcing. Further outsourcing by the Sub Processor is not permitted.

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

6. Right of Data Subject

6.1 Data Subject Request. To the extent permitted by law, Service Provider will inform the 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 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.

6.2 Customer and Service Provider shall cooperate, on request, with the supervisory authority in the performance of its tasks. Customer shall be informed without undue delay of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Agreement. This also applies insofar as Service Provider is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Agreement. Insofar as the Customer is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by Service Provider, the Service Provider shall make every effort to support the Customer.

7. Security

7.1 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.

7.2 Technical and Organizational Measures. Before the commencement of processing, Service Provider shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the awarding of the Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Customer for inspection. Upon acceptance by the Customer, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Customer shows the need for amendments, such amendments shall be implemented by mutual agreement.

Service Provider shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as

the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Exhibit 2]

The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permissible for Service Provider to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented. Service Provider shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of Applicable Law and the protection of the rights of the data subject.

7.3 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.

7.4 Security Incident and Personal Data Breach Management and notifications. Service Provider shall assist Customer in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. Service Provider will notify Customer without undue delay in writing after becoming aware of any violation of any provision of this DPA or any actual or suspected theft or unauthorized Processing, loss, use, disclosure o 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 Law or which Service Provider is required to notify to Customer under Applicable 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 non Launchmetrics-related Products or Force Majeure.

7.5 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 Laws. 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 an 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 make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it

cannot avoid, to minimize) any damage, injury or disruption to Service Provider or the Sub Processor's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. 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.

8. General Terms

8.1 Jurisdiction. This Processing Agreement shall be subject to the exclusive jurisdiction of the Courts of Munich.

8.2 Changes in Applicable Laws. Customer may propose any other variations to this Processing Agreement which Customer reasonably considers to be necessary to address the requirements of any Applicable Laws or any updates of such Applicable Laws. If Customer gives notice for variation, Service Provider shall promptly co-operate (and ensure that any affected Sub Processors promptly co-operate) to ensure that equivalent variations are made to any applicable agreement. If Service Provider gives notice under this section, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Service Provider's notice as soon as is reasonably practicable.

8.3 Judicial Access. Subject to Applicable Laws, 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.

8.4 Severance. Should any provision of this Processing Agreement be invalid or unenforceable, then the remainder of this Processing Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

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 Processing: Service Provider will Process Personal Data to perform the Services pursuant to the Agreement. For further information regarding the Processing related to a particular Service, please see the online Privacy Policy applicable to the Services. The legal basis of the Processing is the execution of the Service Provider Agreement and for legitimate purposes relating to the operation, support and/or use of the Services, such as billing, account management, technical support, product development, and sales and marketing.

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 by Applicable Laws.

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
Title
Contact information (i.e. company, email...)
ID Data
Social media Data
Professional life Data (i.e. position, employer)
Localisation data
Personal life Data (i.e. birthdates)
Payment Data
Other

User Data

Connection Data (i.e. login)
Usage 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

A Data Subject has the right to:

- access to his/her Personal 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 email addresses: support@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. Thirty (30) days of

2.4. 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. Prosodie 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 the AWS and Prosodie Data centre is only allowed to authorized employees over a secure VPN connection.

4. Office Network.

4.1. The office network is protected by Cisco Firewall. Only authorised access is permitted. Documents are shared only among authorised employees.

4.2. 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 Sub Processors

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 request only)	Cloud Service Provider	Ireland

Service Specific Subprocessors

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