ARTESIAN DATA PROCESSING ADDENDUM

1. BACKGROUND

1.1 You (the "**Customer**") and Artesian ("**Artesian**", "**we**", "**our**" or "**us**") entered into an Agreement, comprising the Terms of Service and the Order Form, for the provision of the Services.

1.2 This Data Processing Addendum (the "**DPA**") shall be supplemental to the Agreement and apply to the Processing of Customer Personal Data. In the event of a conflict between any of the provisions of this DPA and the provisions of the Terms of Service, the provisions of this DPA shall prevail.

1.3 This DPA is between the Customer and Artesian (each a "**Party**" and collectively the "**Parties**").

2. DEFINITIONS

2.1 Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement, and the following capitalised terms used in this DPA shall be defined as follows:

(a) "**Controller**" has the meaning given in the GDPR.

(b) "**Data Protection Laws**" means the GDPR, any applicable national implementing legislation including the Data Protection Act 2018, and in each case as amended, replaced or superseded from time to time, and all other applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of Customer Personal Data.

(c) "**Data Subject**" has the meaning given in the GDPR.

(d) "**Processing**" has the meaning given in the GDPR, and "**Process**" will be interpreted accordingly.

(e) "**Processor**" has the meaning given in the GDPR.

(f) "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Personal Data.

(g) **"Standard Contractual Clauses"** means the Standard Contractual Clauses (processors) approved by European Commission Decision C(2010)593 or any subsequent version thereof released by the European Commission (which will automatically apply).

(h) "**Subprocessor**" means any Processor engaged by us who agrees to receive from us Customer Personal Data.

(i) "**Supervisory Authority**" has the meaning given in the GDPR.

3. DATA PROCESSING

3.1 **Instructions for Data Processing.** We will only Process Customer Personal Data in accordance with:

(a) the Agreement, to the extent necessary to provide the Services to you; and

(b) your written instructions,

unless Processing is required by European Union or Member State law to which we may be subject, in which case we shall, to the extent permitted by European Union or Member State law, inform the Customer of that legal requirement before Processing that Customer Personal Data.

3.2 Processing outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and us on additional instructions for Processing.

3.3 **Required consents.** Where required by applicable Data Protection Laws, the Customer will ensure that the Customer has obtained/will obtain all necessary consents for the Processing of Customer Personal Data by us in accordance with the Agreement.

4. TRANSFER OF PERSONAL DATA

4.1 **Authorised Subprocessors.** The Customer agrees that we may use the following as Subprocessors to Process Customer Personal Data:

(a) Full Contact Inc.;
(b) Microsoft Corporation;
(c) Microsoft Ireland Operations Limited;
(d) Callidus Software Inc.;
(e) Zendesk, Inc.;
(f) Oracle Corporation UK Limited;
(g) Cisco Systems, Inc.;
(h) GetGo Technologies UK Limited, a subsidiary of LogMeIn, Inc.;
(i) Salesforce.com, Inc;
(j) SurveyMonkey Europe UC;
(k) Eventbrite, Inc;
(l) Google Inc.;
(m) WordPress.org;
(n) WP Engine, Inc. and
(o) Docusign Inc.

4.2 The Customer agrees that we may use Subprocessors to fulfil our contractual obligations under the Agreement. We shall notify the Customer from time to time of the identity of any new Subprocessors we engage. If the Customer (acting reasonably) has a legitimate reason that relates to a new Subprocessor's Processing of Customer Personal Data, the Customer may object to our use of the new Subprocessor by notifying us in writing within

30 days after receipt of our notice. If the Customer objects to our use of a new Subprocessor, the Parties will come together in good faith to discuss a resolution. If the Customer's objection remains unresolved 30 days after it was raised, either Party may terminate the Agreement. If the Customer's objection remains unresolved 60 days after it was raised, and we have not received any notice of termination, the Customer is deemed to have accepted the Subprocessor.

4.3 Save as set out in clauses 4.1 and 4.2, we shall not permit, allow or otherwise facilitate Subprocessors to Process Customer Personal Data without your prior written consent and unless we enter into a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of Customer Personal Data, as are imposed on us under this DPA.

4.4 **Liability of Subprocessors**. We will at all times remain responsible for compliance with our obligations under the DPA and will be liable to the Customer for the acts and omissions of any Subprocessor as if they were our acts and omissions.

4.5 **Transfers of Personal Data.** To the extent that the Processing of Customer Personal Data by us involves the export of such Customer Personal Data to a third party in a country or territory outside the European Economic Area ("EEA"), other than (i) to a country or territory ensuring an adequate level of protection for the rights and freedoms of Data Subjects as determined by the European Commission; or (ii) where such third party is a member of a compliance scheme recognised as offering adequate protection for the rights and freedoms of Data Subjects as determined by the European Commission, such export shall be governed by the Standard Contractual Clauses between the Customer as exporter and such third party as importer. For this purpose, the Customer appoints Artesian as its agent with the authority to complete and enter into the Standard Contractual Clauses as agent for the Customer on its behalf for this purpose.

5. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

5.1 **Artesian Security Obligations**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the measures set out in Annex 2.

5.2 **Security Audits**. The Customer may, upon reasonable notice, audit (by yourself or using independent third party auditors) Artesian's compliance with the security measures set out in this DPA (including the technical and organisational measures as set out in Annex 1), including by conducting audits of Artesian's data processing facilities.

5.3 Upon your request, we will make available all information reasonably necessary to demonstrate compliance with this DPA.

5.4 **Security Incident Notification.** If we or any Subprocessor become aware of a Security Incident we will (a) notify the Customer of the Security Incident within 72 hours, (b) investigate the Security Incident and provide such reasonable assistance to the Customer

(and any law enforcement or regulatory official) as required to investigate the Security Incident, and (c) take steps to remedy any non-compliance with this DPA.

5.5 **Artesian Employees and Personnel.** We will treat the Customer Personal Data as the Confidential Information of the Customer, and shall ensure that any employees or other personnel have agreed in writing to protect the confidentiality and security of Customer Personal Data.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1 **Data Subject Requests**. Save as required (or where prohibited) under applicable law, we will notify the Customer of any request received by us or any Subprocessor from a Data Subject in respect of their personal data included in the Customer Personal Data, and will not respond to the Data Subject.

6.2 We will provide the Customer with the ability to correct, delete, block, access or copy the Customer Personal Data in accordance with the functionality of the Services.

6.3 **Government Disclosure.** We will notify the Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency.

6.4 **Data Subject Rights.** Where applicable, and taking into account the nature of the Processing, we will use all reasonable endeavours to assist the Customer by implementing any other appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of your obligation to respond to requests for exercising Data Subject rights laid down in the GDPR.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1 To the extent required under applicable Data Protection Laws, we will provide reasonable assistance to the Customer with regard to any data protection impact assessments conducted and any prior consultations made to any Supervisory Authority, in each case solely in relation to Processing of Customer Personal Data and taking into account the nature of the Processing and information available to us.

8. TERMINATION

8.1 **Deletion of data**. Subject to 8.2 and 8.3 below, we will, within 90 (ninety) days of the date of termination of the Agreement:

(a) return or otherwise make available for retrieval a complete copy of all Customer Personal Data; and

(b) delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Data Processed by us or any Subprocessors.

8.2 Subject to section 8.3 below, the Customer may in its absolute discretion notify us in writing within 30 (thirty) days of the date of termination of the Agreement to require us to delete and procure the deletion of all copies of Customer Personal Data Processed by us. We will, within 90 (ninety) days of the date of termination of the Agreement:

(a) comply with any such written request; and

(b) use all reasonable endeavours to procure that our Subprocessors delete all Customer Personal Data Processed by such Subprocessors,

and, where this section 8.2 applies, we will not be required to provide a copy of the Customer Personal Data to you.

8.3 We and our Subprocessors 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 we 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.

ANNEX 1

DETAILS OF THE PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) of the GDPR.

Subject matter and duration of the Processing of Subscriber Personal Data

The subject matter and duration of the processing are as set out in Section 2 and Section 5 of the Agreement, and this DPA.

The nature and purpose of the Processing of Customer Personal Data

The Customer Personal Data will be subject to the following basic processing activities: transmitting, collecting, storing and analysing data in order to provide the Services to the Customer, and any other activities related to the provision of the Services or specified in the Agreement.

The types of Customer Personal Data to be Processed

The Customer Personal Data concern the following categories of data: names; email addresses; business and professional details including current and past employers, job titles, job descriptions, experience and qualifications; geographic locations, and any other personal data provided by the Customer in connection with its use of the Services.

The categories of data subject to whom the Customer Personal Data relates

- Individuals, including Users and any other persons authorised by the Customer to access and use the Services such as employees and independent contractors; and
- Individuals contained in the Customer Personal Data.

Your obligations and rights

Your obligations and rights with respect to the Customer Personal Data are as set out in this DPA.

ANNEX 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Introduction

We maintain internal policies and procedures, or procure that our Subprocessors do so, which are designed to:

- secure any Customer Personal Data Processed by us against accidental or unlawful loss, access or disclosure;
- identify reasonably foreseeable and internal risks to security and unauthorised access to the Customer Personal Data Processed by us;
- minimise security risks, including through risk assessment and regular testing.

We will conduct periodic reviews of the security of our network and the adequacy of our information security program as measured against industry security standards and our policies and procedures, and will use reasonable efforts to procure that our Subprocessors do so as well.

We will periodically evaluate the security of our network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews, and will use reasonable efforts to procure that our Subprocessors do so as well.

Access controls

We limit access to personal data by implementing appropriate access controls.

Availability and back-up of Customer Personal Data

We regularly back-up Customer Personal Data. Back-ups are stored separately and are encrypted at rest.

Disposal of IT equipment

We have in place processes to securely remove all personal data before disposing of IT systems (for example, by using appropriate technology to purge equipment of data and/or destroying hard disks).

Encryption

We use encryption technology where appropriate to protect personal data held electronically.

Transmission or transport of Customer Personal Data

We have implemented appropriate controls to secure Customer Personal Data during transmission or transit.

Device hardening

We remove unused software and services from devices used to process Customer Personal Data. Default passwords that are provided by hardware and software producers will not be used.

Physical security

We implement appropriate physical security measures to safeguard Customer Personal Data.

Staff training and awareness

We carry out staff training on data security and privacy issues relevant to their job role and ensure that new starters receive appropriate training before they start their role.

Staff are subject to disciplinary measures for breaches of our policies and procedures relating to data privacy and security.