Appendix - GDPR (EEA and UK)

During the course of providing Services to, or on behalf of, UC pursuant to the Agreement between UC and Supplier dated _____, Supplier may process personal data as defined below. The Parties agree that with respect to the processing of personal data pursuant to the Agreement or this Appendix – General Data Protection Regulation ("Appendix GDPR"), UC is the data controller (and shall hereinafter be referred to as the "Controller"), and Supplier is the data processor (and shall hereinafter be referred to as the "Processor"), as those terms are defined by the applicable law. The Parties have agreed that the Processor will provide the Services to the Controller pursuant to and in accordance with the terms and conditions of the Agreement and this Appendix GDPR. In the event of a conflict between the terms of this Appendix GDPR and the Agreement or any amendment or appendix thereto, the terms of this Appendix GDPR shall govern. Supplier agrees to be bound by the obligations set forth in this Appendix GDPR. To the extent applicable, Supplier also agrees to impose, by written contract, the terms and conditions contained in this Appendix GDPR on any third party retained by Supplier to provide Services for or on behalf of UC.

A. Definitions

Capitalized terms used but not defined in this Appendix GDPR will have the meanings set forth in the Agreement. The following terms shall have the meanings set forth herein:

1. "Applicable Data Protection Law" means the EU General Data Protection Regulation (Regulation 2016/679) (as may be amended, superseded or replaced); and all other supplemental or implementing laws relating to data privacy in the relevant European member state including where applicable the guidance and codes of practice issued by the relevant supervisory authority; and the UK General Data Protection Regulation;

2. "**Data**" means all personal data processed by (or on behalf of) the Processor for the Controller under or in connection with the Agreement, including in the provision of the Services. If Appendix DS applies to this Agreement, "Data" as used herein shall also be considered UC Institutional Information as defined in Appendix DS.

3. "**Data Subjects' Rights**" means the rights of data subjects as provided in Applicable Data Protection Law including, but not limited to, rights of access, rectification, erasure, restriction of processing, data portability, objection, and the right not to be subject to automated decision making (including profiling);

4. "**EEA**" means European Economic Area;

5. "**data subject**," "**personal data**," "**personal data breach**," "**process/processing**," "**pseudonymisation**," and "**supervisory authority**," shall each have the meaning as in the Applicable Data Protection Law;

6. "**Subprocessor**" means any third party: (i) who is engaged by the Processor to carry out specific processing activities relating to Data for or on behalf of the Controller; or (ii) to whom the Processor subcontracts any of its obligations in connection with the Agreement.

7. "UK" means the United Kingdom.

B. Scope of Processing Data

1. Processor shall process Data solely for the purposes of performing the Services and for the same duration of the Agreement, except as otherwise agreed to in writing by the Parties. The scope and further details of Processor's processing activities of Data pursuant to the Agreement and Appendix GDPR are set forth in Addendum A to this Appendix GDPR.

2. To the extent any additional information is required to be included in Addendum A pursuant to Applicable Data Protection Law, or this Agreement otherwise requires amendment, the Parties will cooperate to amend this Appendix GDPR in a writing signed by both Parties.

C. <u>Subprocessors</u>

1. Controller generally authorizes Processor to engage Subprocessor(s) to perform any of Processor's obligations in providing Services to Controller in connection with the Agreement as set forth in Addendum A and as allowed under the terms of the Agreement, except that any processing of personal data by Subprocessor(s) outside of the United States, UK or EEA must be specifically authorized in writing prior to such processing by Controller.

2. The Processor shall give the Controller prior written notice of any intended changes concerning the addition or replacement of any Subprocessors set forth in Addendum A to allow the Controller to approve or object to such changes. Such notice shall include details of the processing activity or activities to be conducted by the applicable Subprocessor and the identity and contact details of such Subprocessor.

3. The Processor shall ensure that any Subprocessor approved by Controller in accordance with this Section C is subject to obligations in a written agreement requiring such Subprocessor to comply with the obligations of this Appendix GDPR. If any Subprocessor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the performance or non-performance of such Subprocessor.

4. Upon request, the Processor shall provide a copy of each Subprocessor agreement entered into pursuant to this Section C to the Controller.

D. <u>Obligations of the Processor</u>

1. The Processor shall, and shall ensure that each of its employees, approved Subprocessors and any other individual acting under its authority who has access to the Data:

   a. process Data in accordance with the terms of this Agreement, Appendix GDPR or any other written instructions of the Controller, and only to the extent and in the manner necessary to provide Services, and for no other purpose(s). In the event Applicable Data Protection Law requires Processor to process in a manner not expressly authorized by this Agreement or the Controller's written instructions, the Processor shall promptly inform the Controller of the applicable legal requirement before processing, unless prohibited from doing so on important public interest grounds, consistent with Applicable Data Protection Law;

   b. keep the Data confidential and ensure that any person authorized to process the Data for or on behalf of the Processor (including but not limited to any Processor employees and

staff and approved Subprocessors) has agreed to keep the Data confidential, or is otherwise under a statutory obligation to protect the confidentiality of the Data; and

c. upon reasonable request from the Controller, provide an up-to-date copy of the Data in the format requested by the Controller.

2. In carrying out its obligations under the Agreement and this Appendix GDPR, Processor agrees to comply with all applicable state, federal and laws of other countries or jurisdictions (including, but not limited to, Applicable Data Protection Law), as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Data.

3. In accordance with Applicable Data Protection Law, and taking into consideration the state of the art, costs of implementation and the nature, scope, context and purposes of processing the Data pursuant to this Agreement, as well as the risks to the rights and freedoms of natural persons and the risks to processing the Data, the Processor represents and warrants that it has implemented appropriate technical and organizational security measures appropriate to such risks, including, as appropriate: (i) the pseudonymisation and encryption of the Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability of and access to the Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Upon Controller's request, Processor shall provide to Controller evidence demonstrating Processor's implementation of such technical and organizational security measures as required by Applicable Data Protection Law.

4. The Processor shall assist the Controller in ensuring compliance with Controller's obligations as a Controller by: (a) cooperating with Controller's implementation of appropriate technical and organizational security measures to ensure the security of processing Data; (b) cooperating with Controller notifications to supervisory authorities and/or data subjects, as applicable, of any breaches of Data; (c) cooperating with Controller's conduct of data protection impact assessments, including but not limited to, any requirements to consult with a supervisory authority as required by Applicable Data Protection Law. Processor shall also cooperate with additional obligations of Controller that may be required of it pursuant to Applicable Data Protection Law.

5. In the event of any suspected or actual personal data breach, the Processor shall notify the Controller to the individual identified below immediately upon discovery, both orally and in writing, but in no event more than two (2) calendar days after Processor identifies or reasonably believes a personal data breach has or may have occurred. Processor's notification to the Controller will identify: (i) the nature of the personal data breach, including where possible, the categories and the approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) a description of the likely consequences of the personal data breach; and (iii) a description of the measures taken or proposed to be taken to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects. Processor will provide such other information as reasonably requested by Controller. In the event of a suspected personal data breach, Processor will keep Controller informed regularly of the progress of its investigation until the uncertainty is resolved.

In event of suspected or actual personal data breach, the Processor shall notify:

Name		
Phone		
Email		
Address		

6. Processor will fully cooperate with Controller's investigation of any personal data breach, including but not limited to making witnesses and documents available immediately upon Supplier's reporting of the personal data breach at no cost to Controller.

7. Any personal data breach may be grounds for immediate termination of the Agreement by Controller.

8. Except for transfers of Data to the Controller, the Processor shall not process or transfer any Data to any country outside the UK or EEA except pursuant to prior written approval of the Controller, and at all times in compliance with Applicable Data Protection Law and other applicable data protection laws.

9. This section is only applicable if Processor's Services include the collection of personal data directly from data subjects:

   In the event Processor's Services include the collection of personal data directly from data subjects that is to be provided to Controller, unless the parties otherwise agree, the Processor shall be responsible for ensuring that such processing of personal data complies with Applicable Data Protection Law requirements, including, but not limited to, obtaining a lawful basis to process the personal data.

10. This section is only applicable if: (1) Processor or a Subprocessor is based in the UK or EEA; (2) Processor's or such UK- or EEA-based Subprocessor's Services include the transfer of personal data from the UK or EEA to Controller; and (3) data subjects have not explicitly consented to the transfer of their personal data to Controller in the United States:

    Unless the parties otherwise agree on another transfer mechanism that satisfies Applicable Data Protection Law requirements, transfers of personal data shall be governed by the Standard Contractual Clauses set forth in Addendum B to this Appendix GDPR.

11. Processor acknowledges that Controller is subject to U.S. federal and state laws and regulations, including but not limited to public disclosure and retention laws and regulations, that may require the retention and disclosure of information that is the subject of the Agreement.

12. Within thirty (30) days of the termination, cancellation, expiration or other conclusion of this Appendix GDPR, Processor will deliver the Data to UC unless UC requests in writing that such

Data be destroyed. This provision will also apply to all Data that is in the possession of Subprocessors. Such destruction will be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88 Guide to Media Sanitization. Processor will certify in writing to Controller that such delivery or destruction has been completed. In the event Applicable Data Protection Law requires the storage of such Data, the Processor shall promptly inform the Controller of such requirement in writing. In such instance, Processor will continue to protect the Data in accordance with the terms of this Appendix GDPR.

E. <u>Data Subjects' Rights</u>

1. Unless Section D.9 of this Agreement applies, the Controller shall be responsible for providing data subjects with any information required under Applicable Data Protection Law at the time of collecting such data subjects' personal data, as well as any information requested by data subjects relating to the processing of their personal data.

2. The Processor shall notify the Controller (via the individual identified by UC in this Appendix GDPR) in writing (including by e-mail) of each and any request that it receives from a data subject relating to a Data Subject Right. Such written notification shall be made promptly no later than two (2) business days following receipt of the request, and shall include any information in the Processor's custody or control that may assist the Controller to respond to the request.

3. Unless otherwise required by Applicable Data Protection Law, the Processor shall not respond to any such requests or other communications the Processor receives from data subjects, without the prior written consent of the Controller.

4. The Processor shall assist the Controller in Controller's obligations to respond to requests for exercising Data Subjects' Rights by using appropriate technical and organizational measures, to the extent practicable given the nature of the processing of Data.

F. <u>Accountability</u>

1. Upon written request from the Controller, the Processor shall make available to the Controller all information necessary to demonstrate compliance with its obligations under this Appendix GDPR. The Processor shall make its records, documents, facilities, processes and individuals reasonably available to Controller or Controller's designee for audits or inspections to demonstrate compliance with this Appendix GDPR.

2. The Processor shall immediately inform the Controller if, in the Processor's opinion, any instruction from the Controller with respect to the processing of Data pursuant to this Agreement violates or contradicts Applicable Data Protection Law.