Attachment 3
European Union General Data Protection Regulation Terms

The Block Protocol makes the commitments in these GDPR Related Terms, to all customers effective January 1, 2019. These commitments are binding upon the Block Protocol with regard to Customer regardless of (1) the version of the Block Protocol Customer Agreement and DPA that is otherwise applicable to any given Online Services subscription or (2) any other agreement that references this attachment. For purposes of these GDPR Related Terms, Customer and the Block Protocol agree that Customer is the controller of Personal Data and the Block Protocol is the processor of such data, except when Customer acts as a processor of Personal Data, in which case the Block Protocol is a sub-processor. These GDPR Related Terms apply to the processing of Personal Data, within the scope of the GDPR, by the Block Protocol on behalf of Customer. These GDPR Related Terms do not limit or reduce any data protection commitments the Block Protocol makes to Customer in the Block Protocol Customer Agreement or other agreement between the Block Protocol and Customer. These GDPR Related Terms do not apply where the Block Protocol is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. The Block Protocol shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, the Block Protocol shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))

2. Processing by the Block Protocol shall be governed by these GDPR Related Terms under European Union (hereafter "Union") or Member State law and are binding on the Block Protocol with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's licensing agreement, including these GDPR Related Terms. In particular, the Block Protocol shall:

    a. process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Block Protocol is subject; in such a case, the Block Protocol shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

    b. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

    c. take all measures required pursuant to Article 32 of the GDPR;

d. respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;

e. taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

f. assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Block Protocol;

g. at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;

h. make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

The Block Protocol shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

3. Where the Block Protocol engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Related Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, the Block Protocol shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

4. 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, Customer and the Block Protocol shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    a. the pseudonymisation and encryption of Personal Data;

    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

5. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed (Article 32(2)).

6. Customer and the Block Protocol shall take steps to ensure that any natural person acting under the authority of Customer or the Block Protocol who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law (Article 32(4)).

7. The Block Protocol shall notify Customer without undue delay after becoming aware of a Personal Data breach (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to the Block Protocol.