DATA PRIVACY AND PROCESSING ADDENDUM

Revised 8/12/2021

This Data Privacy and Processing Addendum supplements the Agreement between fjorge and its customer who has this data privacy and processing addendum referenced in their master service agreement ("Customer") and addresses the rights and obligations of the parties with respect to data privacy and data processing under Applicable Law.

1. **Definitions.** Capitalized terms which are not defined herein shall have the meaning provided in the Agreement. In addition, the following defined terms apply solely with respect to this Addendum .

    a. "Applicable Law" means any statute, regulation, executive order, and other rule or rules issued by a government office or agency that have binding legal force and are generally applicable to Personal Data or the provision of the Services with respect to Personal Data, including GDPR, CCPA, and the state and federal laws of the United States.
    b. "CCPA" means the California Consumer Privacy Act of 2018.
    c. "Data Subject" means an identified or identifiable natural person whose rights are protected by GDPR or a "Consumer" as defined under CCPA.
    d. "GDPR" means Regulation 2016/679 of the European Parliament.
    e. "Personal Data" means any information about a natural person that is identified or identifiable to the natural person, either alone or in combination with other information, that fjorge will Process or have access to as part of providing the Services, including any such information that is created by means of the Services. Personal Data includes "personal data" as that term is defined under GDPR and "personal information" as defined under the CCPA.
    f. "Process," when used with respect to Personal Data, means: (i) to record, store, organize, structure, analyze, query, modify, combine, encrypt, display, disclose, transmit, receive, render unusable, or destroy, by automated means or otherwise; (ii) to provide cloud or other remote technology hosting services for applications or services that do any of the foregoing; and (iii) any other use or activity that is defined or understood to be processing under Applicable Law.
    g. "Security Event" means any of the following: (i) unauthorized Processing or other use or disclosure of Personal Data; (ii) unauthorized access to or acquisition of Personal Data or the systems on which Personal Data is Processed; (ii) any significant corruption or loss of Personal Data that fjorge is unable to repair within a minimal period of time; (iii) any event that has or is reasonably likely to significantly disrupt the Processing of the Personal Data as part of the Services; and (iv) any material unsuccessful attempt to gain unauthorized access to, or to destroy or corrupt, the Personal Data, but not including any routine, unsuccessful events such as pings, port scans, blocked malware, failed log in attempts, or denial of service attacks.

2. **Confidential Information**. The Personal Data that fjorge Processes for Customer as part of the Services is Customer Confidential Information covered by the confidentiality commitments stated in the Agreement. fjorge agrees to the additional commitments stated in this Addenum as to the Personal Data.
3. **Use and Disclosure**. fjorge will not use, disclose, or Process the Personal Data except as permitted by the Agreement or Customer other written instructions, or as strictly necessary for internal administrative purposes related to the provision of Services. fjorge will make available to Customer list of any sub-processors fjorge uses in compliance with Applicable Law. fjorge will require any sub-processors to contractually agree to terms at least as protective of Customer Personal Data as those stated in this Addendum and the Agreement.
4. **Compliance with Applicable Law**. Each party will comply with Applicable Law as it relates to such party's performance under the Agreement. Customer shall be responsible for compliance with any and all obligations it might have as a Controller and fjorge shall be responsible for compliance with any and all obligations it might have as a Processor, as those terms are defined in any Applicable Law.
5. **Notice of Requests from Data Subjects**. fjorge will promptly notify Customer if fjorge receives a request from a Data Subject to disclose, provide a copy, modify, block, or take any other action with respect to Personal Data pertaining to the Data Subject, unless notice is prohibited by Applicable Law; and, except to the extent required by Applicable Law, fjorge will not independently take any action in response to a request from a Data Subject without Customer prior written instruction. fjorge will cooperate with Customer reasonable requests for access to Personal Data and other information and assistance as necessary to respond to a request or complaint by a Data Subject.
6. **Notification in the event of an actual or suspected Security Event.** In the event of a discovered or suspected Security Event, fjorge shall provide notice without undue delay to Customer's technical and account contacts using those means established for routine account-related communications (or other such method of notice as agreed between the parties). The notice shall include the following information to the extent it is reasonably available to fjorge at the time of the notice, and fjorge shall update its notice as additional information becomes reasonably available: (i) the dates and times of the Security Event; (ii) the facts that underlie the discovery of the Security Event, or the decision to begin an investigation into a suspected Security Event, as applicable; (iii) a description of the Personal Data involved in the Security Event, either specifically, or by reference to the data set(s), and (iv) the measures planned or underway to remedy or mitigate the vulnerability giving rise to the Security Event. fjorge will take reasonable measures to address a vulnerability giving rise to a successful Security Event, both to mitigate the harm resulting from the Security Event and to prevent similar occurrences in the future. fjorge will cooperate with Customer reasonable requests in connection with the investigation and analysis of the Security Event.
7. **Customer Obligations.** Customer represents and warrants that : (i) the Personal Data has been collected in accordance with Applicable Law; (ii) the transfer to fjorge for the purpose of providing the Services is authorized under Applicable Law; (iii)

Customer will comply with Applicable Law as to requests from Data Subjects in connection with the Personal Data; (iv) Customer shall disclose to fjorge only that Personal Data that is necessary for fjorge provision of the Services; and (v) Customer shall not ask fjorge to take any action with respect to the Personal Data that Customer is not permitted to take directly.

8. **CCPA.** For the purposes of CCPA: (i) fjorge is a "Service Provider" as defined under Section 1798.140(v); (ii) Customer is disclosing Personal Data to fjorge solely for a valid business purpose in providing the Services to Customer and (iii) fjorge may not sell Personal Data or retain, use, or disclose Personal Data except as required to provide the Services in accordance with the Agreement.
9. **Audit; Records**. fjorge will comply with any audit request to the extent required by law or due legal process. fjorge will keep reasonable records to evidence our compliance with fjorge obligations under this Addendum and shall preserve such records for at least two (2) years from the date of the events reflected therein.