DATA REQUEST POLICY

On occasion, we may receive requests from government agencies, users, and other third parties to disclose data other than in the ordinary operation and provision of the Services. This Data Request Policy outlines our policies and procedures for responding to such formal requests for data relating to Customers and Authorized Users ("Custodian Data").

I. DEFINITIONS

§ 1.1 Any capitalized terms used in this Data Request Policy that are not defined will have the meaning set forth in the Customer Terms of Service. In the event of any inconsistency between the provisions of this Data Request Policy and the Customer Terms of Service or written agreement with Customer, as the case may be, the Customer Terms of Service or written agreement will control.

II. REQUESTS FOR CUSTOMER DATA BY INDIVIDUALS

§ 2.1 Third parties seeking Customer Data should contact the Customer regarding such requests. The Customer controls the Customer Data and generally gets to decide what to do with all Customer Data.

III. REQUESTS FOR CUSTOMER DATA BY LEGAL AUTHORITY

§ 3.1 We are committed to the importance of trust and transparency for the benefit of our Customers. Except as expressly permitted by the Contract or as described in this policy, we will only disclose Customer Data in response to valid legal process. We require a search warrant issued by a court of competent jurisdiction or the equivalent legal process in the applicable jurisdiction to disclose the contents of Customer Data. We do not voluntarily disclose any data to governmental entities unless

(a) there is an emergency involving imminent danger of death or serious physical injury to any person; or

(b) to prevent harm to the Services or Customers.

We also do not voluntarily provide governments with access to any data about users for surveillance purposes.

§ 3.2 All requests by governmental entities or parties involved in litigation seeking content data associated with Customers who are under contract with us should be sent to **[*email*]**.

§ 3.3 All requests should include the following information:

(a) the requesting party;

(b) the relevant criminal or civil matter; and

(c) a description of the specific Customer Data being requested, including the relevant Customer's name and any relevant Authorized User's name and type of data sought.

§ 3.4 Requests should be prepared and served in accordance with applicable law. All requests should be focused on the specific Customer Data sought. All requests will be construed narrowly by us, so please do not submit unnecessarily broad requests. If legally permitted, Customer will be responsible for any costs arising from our response to such requests.

IV. CUSTOMER NOTICE

§ 4.1 Unless we are prohibited from doing so or there is a clear indication of illegal conduct or risk of harm, we will notify Customer of the request before disclosing any of Customer's Customer Data, so that the Customer may seek legal remedies. If separately agreed with the Customer, the production could be encrypted based on the Customer settings, and may also trigger an observable entry in the access log available to the Customer. If we are legally prohibited from notifying the Customer prior to disclosure, we will take reasonable steps to notify the Customer of the demand after the nondisclosure requirement expires. In addition, if we receive legal process subject to an indefinite non-disclosure requirement, we will challenge that non-disclosure requirement in court.

V. DOMESTICATION AND INTERNATIONAL REQUESTS

§ 5.1 We require that any individual or entity issuing legal process or legal information requests (e.g., discovery requests, warrants, or subpoenas) ensure that the process or request is properly domesticated. For example, for data stored in the Europeean Union, we do not accept legal process or requests directly from law enforcement entities outside the European Union. Foreign law enforcement agencies seeking data stored within the European Union should proceed through a Mutual Legal Assistance Treaty or other diplomatic or legal means to obtain data through a court where we are located.