Sendbird Corporate Customer Data Processing Agreement

Effective as of September 1, 2023

Ver 2.0

Sendbird, Inc. ("Sendbird" or "us" or "our") serves enterprises, public sector entities and other organizations ("Customers") and protects Customer Data in compliance with the terms of this Corporate Customer Data Processing Agreement ("DPA"). "Customer Data" means personal data relating to named or identifiable individuals that Customer's authorized users upload to our servers in compliance with applicable law and our applicable service agreement or other commercial contract terms ("Contract") when Customer's use our remote access software-as-a-service offerings and related data processing services as described in our Instructions and Technical Specifications document as amended from time to time ("Services").

1.   Control and Ownership. The subject matter, nature, purpose and duration of the processing, as well as the types of Customer Data collected and categories of data subjects, are described in Schedule 1 of this DPA. Customers own and control all Customer Data. Sendbird does not use Customer Data, except: (a) in the interest and on behalf of the Customer; (b) as necessary to provide the Services, or (c) as contemplated or directed by the Contract. Sendbird shall notify Customer in the event Sendbird makes a determination that it can no longer meet its obligations under applicable privacy law. Sendbird returns or deletes Customer Data at Customer's request, as agreed in the Contract, or after the Contract expires or is terminated. Sendbird reserves all rights to the Services, Sendbird 's technology and Sendbird's data, including any information that Sendbird discovers, creates or derives as it provides Services, except Customer Data. Customer understands that it is solely responsible for obtaining any needed consents or authorizations for Sendbird to process Customer Data.

2.   Security. Sendbird applies technical, administrative and organizational data security measures that meet or exceed the requirements described in Sendbird's then-current Instructions and Technical Specifications document or published product documentation as applicable (collectively, "TOMS"). Sendbird may update and modify its TOMs from time to time, provided that Sendbird must not reduce the level of security provided thereunder, except with Customer's consent or with 90 days prior written notice (or sooner if required to avoid or mitigate a security incident).

3.   Cooperation with Compliance Obligations. At Customer's reasonable request, Sendbird will (a) reasonably assist Customer with data access, deletion, portability and other requests, subject to compensation for any custom efforts required of Sendbird, and (b) enter into additional contractual agreements to meet specific requirements that are imposed by mandatory laws on Customer pertaining to Customer Data and that, due to their nature, can only be satisfied by Sendbird in its role as service provider or that Customer specifically explains and assigns to Sendbird in an addendum or amendment to the applicable Contract, subject to additional cost reimbursement or fees as appropriate. For the avoidance of doubt, Sendbird shall only assist and enable Customer to meet Customer's obligations to satisfy data subjects' rights, but Sendbird shall not respond directly to data subjects, unless required by law to do so. Additionality, when requested to do so by Customer, Sendbird will promptly make available to Customer all information necessary to assist Customer with its obligations related to conducting a privacy impact assessment. At Customer's request, Sendbird will agree to EU Standard Contractual Clauses for cross-border transfers to processors. If Customer can no longer legally use Sendbird's products due to changes in law or technology, Sendbird shall allow Customer to terminate certain or all contracts and provide transition or migration assistance as reasonably required, subject to termination charges and fees as mutually agreed in good faith by the parties.

4.   Submit to Audits. Sendbird submits to reasonable data security and privacy compliance audits and shares audit report results with Customer. Sendbird also offers a customer audit program subject to reasonable precautions and safeguards for the data of other customers.

5.   Notify Breaches. Sendbird notifies Customer of unauthorized access to Customer Data and other security breaches as required by applicable law.

6.   CCPA Obligations. Sendbird does not accept or disclose any Customer Data as consideration for any payments, services or other items of value. Sendbird does not sell or share any Customer Data, as the terms "sell" and "share" are defined in the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act ("CCPA"). Sendbird processes Customer Data only for the business purposes specified in the written Contract. Sendbird does not retain, use, or disclose Customer Data (a) for cross-context behavioral advertising, or (b) outside the direct business relationship with the Customer. Sendbird does not combine Customer Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA. To the extent Sendbird receives deidentified data from Customer or the Services under the Agreement allow for the deidentification of Customer Data, Sendbird represents

and warrants to not reidentify, attempt to reidentify, or direct any other party to reidentify any data that has been deidentified, unless such services are contemplated under the Contract.

7.   Subprocessors. Customer hereby agrees and provides a general authorization that Sendbird may engage Sendbird's affiliates or third parties as sub-processors to provide the Services. Sendbird will ensure that the sub-processors have entered into a written agreement that is no less protective than this DPA. Sendbird will be fully liable for the acts and omissions of any sub-processors to the same extent as if the acts or omissions were performed by Sendbird. Unless otherwise necessary to protect the security or integrity of Customer Data, in which Sendbird shall promptly provide prior notice, Sendbird shall provide Customer with thirty (30) days prior notice of any additional or replacement sub-processors via our administrative dashboard and our website at https://sendbird.com/sub-processors. After being notified, Customer must notify Sendbird in writing (email shall suffice) withing five (5) days of any reasonable objection it has to such sub-processors. In the event Customer provides a reasonable objection, Sendbird will use commercially reasonable efforts to make a change in processing under the Contract to avoid processing of Customer Data by such sub-processors. If Sendbird is unable to make available such change within a reasonable period of time, Customer may terminate the Services provided under the Contract in respect only to those services which cannot be provided by Sendbird without the use of the objected-to sub-processors, by providing written notice to Sendbird.

8.   Confidentiality. Without prejudice to any existing contractual arrangements between the parties, Sendbird will treat all Customer Data as confidential and it will inform all its employees, agents and any approved sub-processors engaged in processing the Customer Data of the confidential nature of the Customer Data. Sendbird will ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

9.   EEA Personal Data. With respect to any Customer Data that is subject to the EU General Data Protection Regulation (GDPR) or similar laws of other countries as "personal data," Sendbird, in addition to the obligations above, accepts the following obligations as a data importer, processor or subprocessor of Customer:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or EU Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; also, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR, national data protection laws in the EU or other applicable law;

(b) takes all measures required pursuant to Article 32 of the GDPR (security of processing);

(c) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;

(d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

10.   Integration. This DPA is binding on Sendbird if and to the extent it is expressly agreed or incorporated by reference in a duly signed Contract. This DPA shall not create third party beneficiary rights. Sendbird does not accept or submit to additional requirements relating to Customer Data, except as specifically and expressly agreed in writing with explicit reference to the Contract and this DPA. To the extent of applicable law, any claims brought under, or in connection with, this DPA, shall be subject to the exclusions and limitations of liability set forth in the Contract.

Schedule 1 – Details of Processing

Subject Matter	The context for the processing of Customer Data is Sendbird's provision of the Services.
Categories of Customer Data	Customer Personal Data contained in, communication content, traffic data, End-User data, and customer usage data. Communication content, which may include Personal Data or other

	personalized characteristics, depending on the communication content as determined by you as the Customer. Traffic data, which may include Customer Personal Data about the routing, duration or timing of a message, whether it relates to an individual or a company. End-User data, such as any identifier used in setting up and sending messages. Customer usage data, may contain data that can be linked to you as an individual included in statistical data and information related to your account and service activities, service related insights and analytic reports regarding communication sent and customer support. Sensitive data may, from time to time, be processed via the Services where you or your End-Users choose to include sensitive data within the communications that are transmitted using the Services. You are responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting your End-Users to transmit or process any sensitive data via the Services
Categories of Data Subjects	Customer's contact persons (natural persons) or employees, contractors or temporary workers (current, prospective, former) using the Services through the Customer's account ("Users");End-Users. Any individual (i) whose contact details are included in the Customer's contacts list(s); (ii) whose information is stored on or collected via the Services, or (ii) to whom Customer sends communications or otherwise engage or communicate with via the Services (collectively, "End-Users"). You as the Customer solely determine the categories of data subjects included in the communication sent through our Services.
Nature and Purpose of Processing	For the nature and purposes required to provide the Services, as set forth in the Contract.
Duration of Processing	Duration of performance of the Services.