Sendbird's Data Processing Terms

This Data Processing Addendum ("Addendum"), is made as of the last date of signature below ("Effective Date"), between Sendbird, Inc., a Delaware corporation, with its principal place of business at 400 1st, Ave. San Mateo, CA 94401, USA ("Company" or "Sendbird") and [CUSTOMER], with its principal place of business at [ADDRESS] ("Customer"). All capitalized words not defined in this Addendum will have the meaning set forth in the Agreement. The parties agree to comply with the following provisions with respect to any Personal Data (defined below) processed by Sendbird for Customer in connection with the provision of the Services under the Agreement. This Addendum is incorporated by reference into the Agreement between Company and Customer dated on or about [insert date] ("Agreement") and replaces any previously executed Data Processing Addendum executed by the parties. In the event of a conflict between the terms of the Agreement and this Addendum, the terms of this Addendum will control.

1 DEFINITIONS

1.1 "**Affiliates**" means any entity which is controlled by, controls, or is in common control with one of the parties.

1.2 "**Data Controller**" means the entity which determines the purposes and means of the processing of Personal Data.

1.3 "**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.

1.4 "**Data Protection Laws**" means all privacy and data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including, as applicable: (a) the GDPR; (b) applicable data protection law in the United Kingdom (solely to the extent that the United Kingdom is no longer deemed part of the European Economic Area); (c) the Federal Data Protection Act of 19 June 1992 (Switzerland); and/or (d) the California Consumer Privacy Act ("CCPA") and applicable to the Processing of Personal Data under the Agreement.

1.5 "**Data Subject**" means the individual to whom Personal Data relates.

1.6 "**Effective Date**" shall have the meaning ascribed to such term in Section 11.

1.7 "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.8 "**Personal Data**" means any information relating to an identified or identifiable person that is subject to the Data Protection Laws as specified in Appendix 1.

1.9 "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

1.10 "**Security Breach**" has the meaning set forth in Section 7 of this DPA.

1.11 "**Sub-processor**" means any sub-processor engaged by Sendbird for the Processing of Personal Data.

1.12 "**Term**" means the period from the Effective Date to the date the DPA is terminated in accordance with Section 10.1.

2 PROCESSING OF PERSONAL DATA

2.1 To the extent the Services involves the Processing of Personal Data, the parties agree that Customer is the Data Controller and Sendbird is a Data Processor and that the subject matter and details of the processing of such Personal Data are described in Appendix 1. To the extent that the data protection legislation of another jurisdiction is applicable to either party's processing of data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that data. Sendbird shall keep a record of all processing activities with respect to the Customer's Personal Data as required under GDPR.

2.2 Each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Personal Data, including but not limited to providing the other party contact details for each party's Data Protection Officer which are accurate and up to date. Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of the Data Protection Laws, and Customer will ensure that its instructions for the Processing of Personal Data shall comply with the Data Protection Laws. If Sendbird believes or becomes aware that any of the Customer's instructions conflict with any Data Protection Laws, Sendbird shall inform Customer. As between the parties, the Customer shall have sole responsibility for determining the legal basis for the processing of Personal Data and (to the extent legally required) obtain all consents from Data Subjects necessary for collection, and Processing of Personal Data in the scope of the Services.

2.3 The objective of Processing of Personal Data by Sendbird is the performance of the Services pursuant to the Agreement. During the Term of this DPA, Sendbird shall only Process Personal Data on behalf of and in accordance with the Agreement and Customer's instructions and shall treat Personal Data as Confidential Information. Customer instructs Sendbird to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement; and (ii) Processing to comply with other reasonable instructions provided by the Customer where such instructions are acknowledged by Sendbird as consistent with the terms of the Agreement. Sendbird may Process Personal Data other than on the instructions of the Customer if it is mandatory under applicable law to which Sendbird is subject. In this situation, Sendbird shall inform the Customer of such a requirement unless the law prohibits such notice.

2.4 To the extent Sendbird will process Personal Data received from or on behalf of Customer that relates to residents of the State of California, or that is otherwise subject to the CCPA in the course of providing the Services, Sendbird agrees that it will not retain, use, sell or otherwise disclose Personal Data other than: (i) for a Business Purpose (as that term is defined under the CCPA) on behalf of Customer and for the specific purpose of performing the Services, or (ii) as may otherwise be permitted for Service Providers, as defined under the CCPA. Sendbird certifies that it understands the restrictions in this Section 2.4 and will comply with them.

3 RIGHTS OF DATA SUBJECTS; DATA DELETION

3.1 Sendbird shall provide reasonable and timely assistance to Customer to enable Customer to respond to (i) any request from a Data Subject to exercise any of its rights under Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (ii) any other correspondence, inquiry or complaint received from a Data Subject in connection with the processing of the Data.

4 Sendbird PERSONNEL

4.1 Sendbird shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data as well as any security obligations with respect to such Data.

4.2 Sendbird will take appropriate steps to ensure compliance with the Security Measures (defined below) by its personnel to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer's Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that any such obligations survive the termination of that individual's engagement with Sendbird.

4.3 Sendbird shall ensure that access to Personal Data is limited to the personnel who require such access to perform the Services.

5 SUB-PROCESSORS

5.1 The customer acknowledges and agrees that Sendbird may engage third-party Sub-processors in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services Sendbird has retained them to provide, and are prohibited from using Personal Data for any other purpose. Sendbird will have a written agreement with each Sub-processor and agrees that any agreement with a Sub-processor will include substantially the same data protection obligations as set out in this DPA.

5.2 A list of Sub-processors is available to the Customer at https://sendbird.com/sub-processors. Sendbird may change the list of such other Sub-processors by no less than 10 business days' notice via the Sendbird user interface. If the Customer objects to Sendbird's change in such Sub-processors, the Customer's sole and exclusive remedy is to delete the Customer's Sendbird account.

5.3 Sendbird shall be liable for the acts and omissions of its Sub-processors to the same extent Sendbird would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6 SECURITY; AUDIT RIGHTS; PRIVACY IMPACT ASSESSMENTS

6.1 Sendbird shall maintain administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of the Customer's Personal Data. Sendbird will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access as described in Appendix 2 (the "Security Measures", available to those with login credentials). As described in Appendix 2, the Security Measures include measures to protect Personal Data; to help ensure ongoing confidentiality, integrity, availability, and resilience of Sendbird's systems and services; to help restore timely access to Personal Data following an incident; and for regular testing of effectiveness. Sendbird may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

6.2 Sendbird will (taking into account the nature of the processing of Customer's Personal Data and the information available to Sendbird) assist Customer in ensuring compliance with any of Customer's obligations with respect to the security of Personal Data and Personal Data breaches applicable to GDPR, including (if applicable) Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing and maintaining the Security Measures in accordance with Appendix 2; and (b) complying with the terms of Section 7 of this DPA.

6.3 No more than once per year, Customer may engage a mutually agreed-upon third party to audit Sendbird solely for the purposes of meeting its audit requirements pursuant to Article 28, Section 3(h) of the General Data Protection Regulation ("GDPR"). To request an audit, the Customer must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Audit requests must be sent to compliance at compliance@Sendbird.com. The auditor must execute a written confidentiality agreement acceptable to Sendbird before conducting the audit. The audit must be conducted during regular business hours, subject to Sendbird's policies, and may not unreasonably interfere with Sendbird's business activities. Any audits are at Customer's expense.

6.4 Any request for Sendbird to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required by law. The customer shall reimburse Sendbird for any time spent for any such audit at the rates agreed to by the parties. Before the commencement of any such audit, Customer and Sendbird shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Sendbird.

6.5 The customer shall promptly notify Sendbird with information regarding any non-compliance discovered during the course of an audit.

7 SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 If Sendbird becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any of Customer's Personal Data transmitted, stored, or otherwise Processed on Sendbird' equipment or facilities ("Security Breach") which, in the reasonable opinion of Sendbird's Data Protection Officer, requires such notification, Sendbird will promptly notify Customer of the Security Breach. Notifications made pursuant to this section will describe, to the extent possible, details of the Security Breach, including steps taken to mitigate the potential risks and steps Sendbird recommends Customer take to address the Security Breach.

7.2 The customer agrees that an unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Customer's Personal Data or to any of Sendbird's equipment or facilities storing Customer's Personal Data and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, or similar incidents.

7.3 Notification(s) of Security Breaches, if any, will be delivered to the Customer's business, technical or administrative contacts by any means Sendbird selects, including via email. It is the Customer's sole responsibility to ensure it maintains accurate contact information on Sendbird's support systems at all times.

7.4 Sendbird's notification of or response to a Security Breach under this Section 7 will not be construed as an acknowledgment by Sendbird of any fault or liability with respect to the Security Breach.

7.5 Sendbird shall implement reasonable technical and organizational Security Measures to provide a level of security appropriate to the risk in respect to the Customer's Personal Data. As technical and organisational measures are subject to technological development, Sendbird is entitled to implement alternative measures provided they do not fall short of the level of data protection set out by Data Protection Law.

7.6 Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of the processing of Customer's Personal Data as well as the risks to individuals) the Security Measures provide a level of security appropriate to the risk in respect to Customer's Personal Data.

8. RETURN AND DELETION OF YOUR DATA

8.1 Sendbird will enable Customers to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an instruction to Sendbird to delete the relevant Personal Data from Sendbird's systems in accordance with Data Protection Laws. Sendbird will comply with instructions from the Customer to delete certain Personal Data as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) requires further storage.

On the expiry of the Agreement, Customer instructs Sendbird to delete all of Customer's Personal Data (including existing copies) from Sendbird's systems and discontinue processing of such data in accordance with Data Protection Law. Sendbird will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) requires further storage. This requirement shall not apply to the extent that Sendbird has archived Customer's Personal Data on backup systems so long as Sendbird securely isolates and protect such data from any further processing except to the extent required by applicable law. Without prejudice to this Section, Customer acknowledges and agrees that Customer will be responsible for exporting, before the Agreement expires, any of Customer's Personal Data Customer wishes to retain afterward. Notwithstanding the foregoing, the provisions of this DPA will survive the termination of this Agreement for as long as the Sendbird retains any of the Customer's Personal Data.

9 CROSS-BORDER DATA TRANSFERS

9.1 Sendbird may, subject to this Section 9, store and Process the relevant Personal Data in the European Economic Area, Switzerland, the United Kingdom, and the United States.

9.2 If the Services involve the storage and/or processing of Customer's Personal Data which transfers such Personal Data out of the European Economic Area or Switzerland to a jurisdiction that does not have adequate Data Protection Laws, and the Data Protection Laws apply to the transfers of such data ("Transferred Personal Data"), the parties agree that the EU Commission Implementing Decision (EU) 2021/914 and available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (as amended or updated from time to time) ("**Standard Contractual Clauses**") will apply and such Standard Contractual Clauses shall be incorporated by reference and form an integral part of this DPA. Purely for the purposes of the descriptions in the Standard Contractual Clauses and only as between Customer and Sendbird, the parties agree that: (a) Roles of the Parties: Customer is a Data Controller and "data exporter" and Sendbird is the Data Processor and "data importer" under the Standard Contractual Clauses, (b) Governing Law and Supervisory Authority: The Standard Contractual Clauses shall be governed by the law of the EU Member State in which the data exporter is established and enforced by the Supervisory Authority of such EU Member State. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of an EU Member State that does allow for third-party beneficiary rights. In such case, the Parties agree that this shall be the law of _____ (specify Member State); (c) Sub-Processors: the parties select general written authorization for Sub-processors; (d) Redress: The parties elect to omit the optional text; and (e) Annex I, II and III are provided at the end of this DPA as Appendix A and to the extent that there's a conflict as between the DPA and the Appendix A, the Appendix A shall govern.

9.3 The parties further agree that if Transferred Personal Data includes Personal Data from Data Subjects located in the United Kingdom, the parties will safeguard such data using mechanisms which are equivalent to those of the Standard Contractual Clauses until such time as the United Kingdom formally approves a set of UK Standard Contractual Clauses at which point the parties shall execute the UK standard Contractual Clauses.

9.4 At Customer's written request, or if the Services involve the storage and/or processing of Customer's Personal Data collected from persons located in Argentina, Brazil or another jurisdiction not described above but which restricts the transfer of such Personal Data (each a "Restricted Transfer Country") outside of each Restricted Transfer Country to a place that does not have adequate data protection laws, the parties agree to execute each applicable Restricted Transfer Country's model clause agreement.

9.5 To the extent Customer is the recipient of Personal Data from Sendbird pursuant to this DPA, Customer agrees that Customer will provide at least the same level of protection for the information as Sendbird has agreed to provide herein.

9.6 If the Standard Contractual Clauses or any other model clause transfer agreement are deemed invalid by a governmental entity with jurisdiction over Transferred Personal Data (e.g., the EU Court of Justice) or if such governmental entity imposes additional rules and/or restrictions regarding such Transferred Personal Data, the parties agree to work in good faith to find an alternative and/or modified approach with respect to such Transferred Personal Data which is in compliance with applicable laws.

10 LIABILITY

10.1 Both parties agree that their respective liability under this DPA shall be apportioned according to each parties' respective responsibility for the harm (if any) caused by each respective party.

10.2 Liability Cap Exclusions. Nothing in this Section 10 will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

11 MISCELLANEOUS

11.1 This DPA will take effect on the date indicated below (the "Effective Date") and will remain in effect until, and automatically expire upon, the deletion of all of the Customer's Personal Data by Sendbird as described in this DPA.

11.2 Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

11.3 Where Customer's Affiliates are Data Controllers of the Personal Data, they may enforce the terms of this DPA against Sendbird directly.

11.4 This DPA may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one Agreement.

EXECUTED by and on behalf of:	**EXECUTED by and on behalf of:**
Sendbird, Inc.	**[*CUSTOMER*]**

…….	…….
Name	**Name**
…….	…….
Date	**Effective Date**

APPENDIX A

ANNEX I

A. LIST OF PARTIES

Data exporter: The data exporter is the **Customer**

Data importer: The data importer is **Sendbird, INC.**, a company focused on enabling a chat and messaging Application Programming Interface (API), Software Development Kits (SDK), and a fully managed server infrastructure, namely the White Label Chat API Services, to record, transcribe and store the output of an online chat, including the content, participants and any associated documentation.

B. DESCRIPTION OF TRANSFER

Data subjects:

The personal data transferred concerns the following categories of data subjects: Data exporter's customers and end-users.

Categories of data:

The data exporter determines and controls what data it requires from its users. This data, may or may not include personal data as determined by the data exporter. The data importer will receive all categories of data exchanged by various uses of the Sendbird Service, such as text, message, voice, video, images, and sound provided by the data exporter in Sendbird's cloud communications products and services.

Special categories of data (if appropriate):

The personal data transferred regarding the following special categories of data: Sendbird does not intentionally collect or process any special categories of data in the provision of its products and/or services. However, special categories of data may from time to time be inadvertently processed by Sendbird where the data exporter or its end users choose to include this type of data within the communications it transmits using Sendbird products and/or services. As such, the data exporter is solely responsible for ensuring the legality of any special categories of data it or its end users choose to process using Sendbird's products and/or services.

Processing operations

All personal data transferred will be subject to the following basic processing activities in order for Sendbird to provide the Services as outlined in the Agreement: the provision of programmable communication products and services, primarily offered in the form of APIs, on behalf of the data exporter, including transmittal to or from the data exporter's software application from communications networks.

C. COMPETENT SUPERVISORY AUTHORITY

The Standard Contractual Clauses shall be governed by the law of the EU Member State in which the data exporter is established and enforced by the Supervisory Authority of such EU Member State.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Service Infrastructure Management:

- Physical Security: Sendbird has a security program that manages visitors, office entrances, and information assets across geographically distributed offices. Sendbird takes advantage of AWS data centers for all production systems and customer data. Our infrastructure management is designed and built on AWS's security policies.

- Network Security: Sendbird has established procedural and technical standards for deploying network functions to production. These standards include baseline configurations for network components, network architecture, and approved protocols and ports. All network components are monitored to prevent malicious activities that might affect the company's infrastructure and to maintain compliance with technical standards. Using a virtual private network (VPN) and the trusted firewalls, Sendbird keeps the service environment safe and secure from external threats and vulnerabilities.

- Cloud Security: The Sendbird service is hosted on AWS which offers state-of-the-art physical protection for the servers and related infrastructure that comprise the service environment. AWS geographic regions and Auto Scaling allows Sendbird to build a highly resilient service for clients. It also allows Sendbird to manage the production servers so that they remain operational against the effects of unexpected events such as natural disasters and local outages.

- Monitoring: Sendbird's monitoring program focuses on detecting and reporting vulnerabilities in our service and products. All system changes and vulnerabilities are monitored and audited with AWS Cloudtrail and AWS GuardDuty. Based on inbound security reports, our engineers quickly analyze vulnerabilities, find the best solutions, and resolve issues.

- Audit Log: Sendbird only grants authorized employees access to customer data based on the principle of least privilege. They are required to use proprietary monitoring tools to detect intrusion attempts and other security-related alerts and to record audit logs for their activities. Audit logs are maintained for all operations and activities such as privileged user access and unauthorized access attempts of customer data.

3. Access Security

- Authentication - MFA, OTP: Access to customer data is restricted to authorized employees. Sendbird applies multi-factor authentication (MFA) and controls for administrative access to its system. For secure authentication, employees are required to use a proprietary VPN solution with MFA when accessing the system. And upon a data owner's request and approval, temporary access to customer data is granted to only a limited group of employees by using a one-time password. All related activities are tracked by audit logs. Access to the company's system and customer data requires two-factor authentication according to the following criteria: a unique user ID, strong password, OTP, and/or certificate.

- Password Management: Employees are required to change passwords regularly according to the Sendbird Password Policy. The policy defines and configures the corporate password requirements including complexity, length, history, and duration.
- Endpoint Management: The Trust and Safety team monitors, manages and restricts all workstations and mobile devices that are used to access the company's system. All workers - regular employees and independent contractors - must install an endpoint protection agent that consists of anti-malware, intrusion prevention, and a firewall. Endpoint protection has an administrative console that allows the Trust and Safety team to monitor any employee's access and events within the Sendbird system environment.

4. Change Management

- Development: In the event of software releases, the company uses a proprietary ticketing system to document procedures for tracking, testing, approving, and validating. A change management project is created when the ticketing system tracks activities from software development and customer requests. Any changed source code is reviewed and approved before it is released to the production environment by using proprietary tools such as GitHub and CircleCI.
- Tracking: All audit logs are recorded for easy tracking of the changes in the ticketing system. The Trust and Safety team regularly checks these logs to make sure procedures comply with system change management. Sendbird also maintains updates to management policies regarding security code reviews and emergency fixes.
- Vulnerability Management: Sendbird operates its own vulnerability management program that actively investigates security vulnerabilities using a combination of automated scans and penetration tests. Automated scans identify all types of vulnerabilities in the software, system, and network components. Once vulnerabilities are identified, the vulnerability management program classifies and remediates vulnerabilities across all Sendbird services. Sendbird also takes corrective actions when necessary, based on the results of our annual penetration tests conducted by an external independent third party.

5. Customer Data Security

- Encryption: Sendbird stores all types of data in the AWS relational database and the data are protected by strong encryption at rest and in transit. AWS provides data-at-rest options and key management to support the encryption process for stored data. Sendbird uses the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols, AES-256 encryption. Data at rest in AWS relational database are also encrypted by AES-256 encryption standards. And also, Sendbird uses the AWS Key Management Service (KMS) for handling the lifecycle of the data encryption key, which applies access controls for the key's generation, usage, and revocation.
- Incident Management: The Trust and Safety team has established protocols and guidelines for responding to emergency security incidents. All incidents are thoroughly investigated, documented, and reported to our Incident Response team for timely mitigation, including suspected or known violations of privacy and security.
- Retention: Sendbird's Data Classification and Protection Matrix classifies customer data into seven categories and defines security controls, handling methods, and retention period for each data category. We provide this paper to customers under a mutual NDA agreement. The contract and service licensing agreement signed between Sendbird and a client sets out the duration of how long Sendbird retains customer data after the termination of the contract. Customer data will be removed from the Sendbird server accordingly.

6. Business Continuity

- Business Continuity Plan: Business Continuity Planning (BCP) has been established for Sendbird services, which provides detailed procedures for recovery and reconstitution of systems known as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). The BCP focuses on monitoring its sub-service organization (AWS), protecting Sendbird employees, and reallocating resources. Our BCP is reviewed on an annual basis.
- Disaster Recovery Drills: The engineering department conducts annual business continuity and disaster recovery drills to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the business continuity and disaster recovery exercise develop drill plans and post-mortems.
- Data Backup Management: All customer data is replicated to protect the availability of Sendbird's services. Data replication occurs within the same region of AWS in which the client's service is hosted. Sendbird typically configures the replication between one primary server and one secondary server within the same region. This replication provides multiple zones of availability. Sendbird uses AWS RDS Multi-AZ deployments to provide availability and durability for database (DB) instances. Upon provisioning a Multi-AZ DB instance, a primary DB instance is automatically created and synchronously replicates the data to a standby instance in a different availability zone (AZ). With reference to data replication, Sendbird services can resume database operations right after failover is completed. Furthermore, Sendbird services operate globally on multiple AWS regions and availability zones within each of those regions. Resources, such as database instances and customer data, are backed up and managed by AWS RDS on a region basis.

Supplemental Measures implemented pursuant to The **European Data Protection Board** (EDPB) Recommendations 01/2020 on measures which supplement Sendbird's transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 and adopted on 18 June 2021 are available upon request.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors listed as of the date of execution of this DPA.

https://Sendbird.com/sub-processors