# Sendbird Corporate Customer Data Processing Agreement

*Effective as of January 19, 2024*

*Ver 3.0*

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. Customer will ensure that its instructions comply with applicable law, including any applicable privacy laws. Customer acknowledges that Sendbird is neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Sendbird's provision of the Services meets or will meet the requirements of such laws or regulations. Customer will ensure that Sendbird's processing of Customer Data, when done in accordance with Customer's instructions, will not cause Sendbird to violate any applicable law or regulation, including applicable privacy laws.

2. Security. Sendbird applies the technical, administrative and organizational data security measures as set forth in Schedule 2 of this DPA (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 and as required by applicable privacy law, Sendbird will (a) reasonably assist Customer with data access, deletion, portability and other requests, subject to compensation for any custom efforts required of Sendbird, (b) assist Customer in ensuring compliance with its obligations under applicable privacy law, including taking into account the nature of processing and the information available to the Sendbird and (c) 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. 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. Unless otherwise prohibited by applicable law, Sendbird notifies Customer of a Security Breach without undue delay after Sendbird confirms a Security Breach. "Security Breach" means a breach of Sendbird's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data in Sendbird's possession, custody or control. Security Breaches do not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

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 and UK Personal Data. With respect to any Customer Data that is subject to the EU General Data Protection Regulation ("EU GDPR") or the UK Data Protection Act 2018 and the UK General Data Protection Regulation ("UK GDPR" and together with the EU GDPR, the "GDPR"), Sendbird, in addition to the obligations in this DPA, will agree, at Customer's request, to enter into the appropriate transfer documentation, including the European Union's Standard Contractual Clauses and the United Kingdom's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses.

10. Deletion of Customer Data. Sendbird shall return and/or delete Customer Data in accordance with the applicable provisions in the Contract.

11. 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. |

**Schedule 2 – Security Measures**

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.

2. 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.

3. 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.

**4.** 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.

**5.** 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.