This Data Processing Agreement applies to you if you signed up for MessageBird's Services (including through any of its Affiliates) before, on, or after 3 May, 2023. Our archived Data Processing Agreement is available here.

Data Processing Agreement

This Data Processing Agreement, including the appendices, ("**DPA**") forms part of the Agreement between MessageBird and Customer for the purchase of (online) communication services from MessageBird to reflect the Parties' agreement with regard to the processing of Customer Personal Data. In this DPA, the terms *"***you***",* *"***your***",* or *"***Customer***"* refer to you (subject to Section 1.2 below), and the terms "**we***",* *"***us***,"* *"***our***"* or *"***MessageBird***"* refer to us. Capitalised terms used in this DPA but not defined below are defined in the MessageBird General Terms and Conditions or other Agreement with us governing your use of the Services.

The parties agree that this DPA will replace any existing data protection addendum or similar agreement the parties may have previously entered into in connection with the Services.

1. Scope, Customer Affiliates and Term

1.1 Scope. This DPA governs processing of Customer Personal Data by MessageBird as a processor.

1.2 Customer Affiliates. Customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Affiliates (as defined in the Terms), if and to the extent you provide such Affiliates with access to the Services and we process Customer Personal Data for which such Affiliates qualify as the data controller ("**Customer Affiliates**"). For the purposes of this DPA only, and except where indicated otherwise, the terms "Customer" and "you" shall include Customer and Customer Affiliates.

1.3 Term. This DPA shall remain in effect so long as MessageBird processes Customer Personal Data subject to this DPA, notwithstanding the expiration or termination of the Agreement.

2. Definitions

"**Account Data"** is any Personal Data provided by or for you to MessageBird in connection with the entering into and administration of the Agreement and of your account, including but not limited to contact information, billing details and correspondence about the entering into and administration of the Agreement and the related Services.
"CCPA" means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time.
"Customer Data" means any data and other information or content submitted by you or for you (or by a user of your Customer Application) under the Agreement and processed or stored by the Services.
"Customer Personal Data" means Personal Data contained in Customer Data processed by MessageBird as a processor, unless otherwise specified in this DPA.
"**Data Protection Laws**" means all laws and regulations of any jurisdiction applicable to the confidentiality, privacy, security, or processing of Personal Data under the Agreement, including, for example and where applicable, the GDPR or the CCPA. .
"EEA" means, for the purposes of this DPA, the European Economic Area and Switzerland.

"**GDPR**" means either (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation); or (ii) solely with respect to the United Kingdom, the Data Protection Act 2018.

"MessageBird" means the MessageBird Entity which is a party to this DPA, being the contracting entity listed in Section 15 in the General Terms and Conditions (Contracting Entity), unless otherwise stated on your Order Form. You or MessageBird may also be referred to individually as a "Party" and together as "Parties" in this DPA.

"**Personal Data**" means any information relating to a directly or indirectly identified or identifiable natural person, whether by itself or in combination with other information.

"**Personal Data Breach**" means any accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to Customer Personal Data and any other similar term under applicable Data Protection Laws such as "Security Breach."

"**Services**" means all products and services provided by us or our Affiliates that are (a) ordered by you under any Order Form; or (b) used by you.

"**Standard Contractual Clauses**" means Controller to Processor (Module Two) or Processor to Processor (Module Three), as applicable, of the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj,.

"**Sub-processor**" means a third party entity that processes Customer Personal Data on behalf of the MessageBird entity acting as a data processor or a Sub-processor.

"**UK Standard Contractual Clauses**" means any or all of the following: (i) international data transfer agreement issued by the UK Information Commissioner under section 119A of the DPA 2018; (ii) the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued by the UK Information Commissioner under section 119A of the DPA 2018; or (iii) such standard contractual provisions issued by the UK Information Commissioner or European Commission as may replace these from time to time.

Terms such as "processing", "data controller", "data processor", "data subject", etc. shall have the meaning assigned to them under the GDPR. The definition of "data controller" includes "business", "consumer", "controller", and "organisation"; "data processor" includes "service provider", "processor", and "data intermediary"; "data subject" includes "consumer", and "individual"; and "Personal Data" includes "personal information", in each case as defined under the CCPA, , and other applicable Data Protection Laws. The terms "business purpose", "commercial purpose", "sell," and "share" shall have the same meaning as in the applicable Data Protection Laws and, in each case, their cognate terms shall be construed accordingly.

3. Processing of Customer Personal Data

3.1 Purposes. We will process Customer Personal Data only to the extent necessary (i) to provide the Services, including transmission of communication, ensuring the security of the services, providing technical and delivery reports, providing support and developing and implementing improvements and updates in accordance with your documented instructions to us as a data processor as specified in Section 3.2 of this DPA, (ii) for our legitimate business purposes as specified in Section 3.4 of this DPA as a data controller, and (iii) as otherwise required under applicable law.

3.2 Customer Instructions. The Agreement and this DPA constitute your complete instructions to us as a data processor at the time of signature of this DPA. We will comply with other reasonably documented instructions provided that those instructions are consistent with the terms of the Agreement.

3.3 Details of Processing. Annex I, Part B (*Description of transfer*) of Appendix I to this DPA specifies the nature and purpose of the processing by us as a data processor or Sub-processor, the processing activities, the duration of the processing, the types of Personal Data, and the categories of data subjects.

3.4 Legitimate Business Purposes. You acknowledge that we process Customer Personal Data as an independent data controller to the extent necessary for the following legitimate business purposes: billing, account management, financial and internal reporting, combatting and preventing security threats, cyber attacks, and cybercrime that may affect you, us or our services, business modelling (e.g. forecasting, capacity and revenue planning, and product strategy), fraud, spam, and abuse prevention and detection, improvement of products or services in the MessageBird suite, and to comply with our legal obligations.

4. Customer Obligations

4.1 Lawfulness. Where you act as a data controller of Customer Personal Data, you guarantee that all processing activities are lawful, have a specific purpose, and any required notices and consents or other appropriate legal basis are in place to enable lawful transfer of the Customer Personal Data. If you are a data processor (in which case we will act as a Sub-processor), you will ensure that the relevant data controller guarantees that the conditions listed in this Section 4.1 are met.

4.2 Compliance. You are solely responsible for (a) ensuring that you comply with the Data Protection Laws applicable to your use of the Services and to your own processing of Customer Personal Data, (b) making an independent assessment whether the technical and organisational measures of the Services meet your requirements, and (c) implementing and maintaining privacy and security measures for components that you provide or control (including but not limited to passwords, devices used with the Services and Customer Applications).

5. Security

5.1 Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we shall implement and maintain appropriate technical and organisational security measures to protect Customer Personal Data from Personal Data Breaches and to preserve the security, integrity, availability, resiliency and confidentiality of the Customer Data our systems use for processing Customer Personal Data. The security measures applied by us are described in Appendix II.

5.2 Updates to Security Measures. You are responsible for reviewing the information made available by us relating to Customer Personal Data security and making an independent assessment as to whether such information meets your requirements and legal obligations under Data Protection Laws. You acknowledge that the security measures are subject to technical progress and development, and that we may update or modify our security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Customer Personal Data.

5.3 Access Controls. We apply the principles of “need to know “and “least privilege” ensuring that access to Customer Personal Data is limited to those Personnel required for the provisioning of the Services and in line with the Agreement, including this DPA.

5.4 Confidentiality of Processing. We will ensure that any person or party who is authorised by us to process Customer Personal Data (including our personnel, agents and Sub-processors) are informed of the confidential nature of such Customer Personal Data and will be under an appropriate obligation of confidentiality (whether a contractual or statutory duty) that survives termination of their engagement.

5.5 Personal Data Breach Response and Notification. Upon becoming aware of a Personal Data Breach, we will without undue delay (i) notify you, (ii) investigate the Personal Data Breach, (iii) provide timely information relating to the Personal Data Breach as it becomes known or as it is reasonably requested by you, and (iv) take commercially reasonable steps to mitigate the effects and prevent recurrence of the Personal Data Breach.

6. Assistance

6.1 Data Protection Assistance. We shall provide you with reasonably requested assistance in order to allow you to comply with your obligations under the Data Protection Laws, including the notification of a Personal Data Breach, assessing the appropriate level security of processing, and assisting you with the performance of a relevant data protection impact assessment.

6.2 Assistance with Rights of Data Subjects. We will provide you with reasonable assistance in order to allow you to comply with your obligations to data subjects who exercise their rights under the Data Protection Laws by making available technical and organisational measures via your account. For the avoidance of doubt, you as the data controller are responsible for processing any request or complaint from data subjects with respect to the Customer Personal Data of a data subject.

7. Disclosure and Disclosure Requests

7.1 Limitations on Disclosure and Access. We will not provide access to or disclose Customer Personal Data except (i) as directed by you, (ii) as set out in the Agreement and this DPA, or (iii) as required by law.

7.2 Disclosure Requests. We will notify you as soon as reasonably possible if we receive a request from a governmental or regulatory body to disclose Customer Personal Data, unless such notice is prohibited by law. We will handle disclosure requests in accordance with the disclosure request policy available at https://messagebird.com/en/legal/disclosure-requests.

8. Sub-processors

8.1 List of Current Sub-processors. You agree to the engagement of the Sub-processors listed at MessageBird's overview of Processors and Subprocessors under the header “End User Personal Data”, which contains a procedure for you to subscribe to notifications of changes to our use of Sub-processors. If you subscribe to such notifications, and taking into account Section 8.3 of this DPA, we will share details of any change in Sub-processors as soon as reasonably possible.

8.2 Appointment of Sub-processors. By means of this DPA, you provide a general written authorization to us to engage Sub-processors for the processing of Customer Personal Data, subject to Section 8.3 of this DPA and the following requirements:

(a) We will restrict access to Customer Personal Data by Sub-processors to what is strictly necessary to provide the services specified in the sub-processor agreement;
(b) We will agree upon data protection obligations with the Sub-processor that are substantially the same as the obligations under this DPA; and
(c) We remain liable to you under this DPA for the performance of the data protection obligations of the Sub-processor.

8.3 **Notification of Changes to Sub-processors and Right to Object**. Before replacing or engaging new Sub-processors (“**Sub-processor Change**”), we will give you the option to object to the Sub-processor Change. You may object to a Sub-processor Change provided that (i) the objection is made in writing within ten (10) business days of our notice of the Sub-processor Change and (ii) the objection is based on

and clearly explains the reasonable grounds relating to the protection of Customer Personal Data. When you object to a proposed Sub-processor Change, we shall work with you in good faith to make a commercially reasonable change in the provision of the Services that avoids the use of the relevant Sub-processor. If such change cannot reasonably be made within thirty (30) business days from our receipt of your objection notice, or if the change is commercially unreasonable for us, either party may terminate the applicable features of the Services which cannot be provided without the use of the relevant Sub-processor. This termination right is your sole and exclusive remedy if you object to a Sub-processor Change.

9. Cross Border Transfers of Customer Personal Data

9.1 Transfers of Customer Personal Data. We may transfer Customer Personal Data on the condition that all appropriate safeguards required by Data Protection Laws are in place. This may include a prior data transfer impact assessment, the adoption, monitoring and evaluation of supplementary technical, organisational and legal measures, enforceable data subject rights, and that effective legal remedies for data subjects are available.

9.2 Sub-processor Standard Contractual Clauses. Unless an adequacy decision or alternative transfer mechanism applies, we have entered into and shall maintain Standard Contractual Clauses with Sub-processors (including our Affiliates) located outside the EEA, subject to the terms set out in Section 9.1 of this DPA.

9.3 Transfer Mechanisms for Customer Personal Data Transfers. To the extent your use of the Services requires a cross border data transfer mechanism to lawfully export Customer Personal Data from a jurisdiction (e.g. the EEA, California, Singapore, Switzerland, or the United Kingdom) to us located outside of that jurisdiction this section will apply. If, in the performance of the Services, Customer Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies to this DPA is transferred to MessageBird located in countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the parties to the extent such transfers are subject to the Data Protection Laws.

9.3.1 The parties agree that the Standard Contractual Clauses will apply to Customer Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to a MessageBird entity located in a country outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data.

9.3.1.1 When you are acting as a data controller and MessageBird is a data processor the EU Controller-to-Processor (Module Two) of the Standard Contractual Clauses will apply to any such transfer of Customer Personal Data from the EEA. When you are acting as a data processor and MessageBird is a sub-processor the Processor-to-Processor (Module Three) of the Standard Contractual Clauses will apply to any such transfer of Customer Personal Data from the EEA.

9.3.1.2 MessageBird will be deemed the data importer and you will be deemed the data exporter under the Standard Contractual Clauses. Each party's signing of this DPA, will be treated as signing of the applicable Standard Contractual Clauses, which will be deemed incorporated into this DPA. Details required under Annex 1 and Annex 2 to the Standard Contractual Clauses are available in Appendix I and Appendix II to this DPA. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail solely with respect to a transfer of Customer Personal Data from the EEA.

9.3.1.3 Where the Standard Contractual Clauses require the parties to choose between optional clauses and to input information, the parties have done so as set out below:

i. The Optional Clause 7 "Docking clause" shall not be adopted.

ii. For Clause 9 "Use of sub-processors", the parties elect the following option: "Option 2 General written authorisation: the data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s)."

iii. For Clause 11 (a) "Redress", the parties do not adopt the Option.

iv. For Clause 17 "Governing law", the parties elect the following option: "Option 1. These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands."

v. For Clause 18 (b) "Choice of Forum and Jurisdiction": "The Parties agree that those shall be the courts of the Netherlands."

9.3.2 The parties agree that the UK Standard Contractual Clauses will apply to Customer Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to a MessageBird entity located in a country outside the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data.

9.3.2.1 MessageBird will be deemed the data importer and you will be deemed the data exporter under the UK Standard Contractual Clauses. Each party's signing of this DPA, will be treated as signing of the UK Standard Contractual Clauses, which will be deemed incorporated into this DPA. Details required under the UK Standard Contractual Clauses are available in Appendix I and Appendix II to this DPA. In the event of any conflict or inconsistency between this DPA and the UK Standard Contractual Clauses, the UK Standard Contractual Clauses shall prevail solely with respect to transfer of Customer Personal Data from the United Kingdom.

10. Audit

10.1 Audit Report. Our communication platform shall be regularly audited against the ISO 27001:2013 standard (or equivalent). The audit may, in our sole discretion, be an internal audit, or an audit performed by a third party. Upon written request, we will provide you with a summary of the audit report(s) ("**Audit Report**"), so that you can verify our compliance with the audit standards and this DPA. Such Audit Reports, as well as any conclusions or findings specified therein, are our Confidential Information.

10.2 Customer information requests. We will make available to you all information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA. We will provide written responses to reasonable requests for information made by you, including responses to information security and audit questionnaires that are reasonable in scope and necessary to confirm compliance with this DPA, provided that you (i) have first made a reasonable effort to obtain the requested information from the Documentation, Audit Reports and other information provided or made public by us, and (ii) will not exercise this right more than once per year, unless a Personal Data Breach or significant change in our processing activities in relation to the Services require that an additional questionnaire is executed. All

responses provided are our Confidential Information.

10.3 Customer Audit. If an Audit Report provided by us to you gives you substantiated reasons to believe that we are in breach of our obligations under this DPA, related to the Customer Personal Data provided by you, we will allow an independent and qualified third party auditor appointed by you and approved by us, to audit the relevant applicable Personal Data processing activities, provided that to the greatest extent permitted under applicable law, the following requirements are met:

(a) You shall give us at least sixty (60) days reasonable advance notice before exercising the right to audit;
(b) The auditor agrees to market standard confidentiality obligations with us;
(c) You and the auditor take measures to minimise disruption to our business operations;
(d) The audit will be carried out during regular business hours;
(e) We shall not be obliged to provide access to customer data of other customers or systems not involved in the provision of the Services; and
(f) You shall pay for all costs of the audit.

11. Deletion and Return of Customer Personal Data. Upon termination or expiration of the Agreement, we will (at your election) delete or return to you all Customer Personal Data (including copies) in our possession or control, save that this requirement will not apply to the extent we are required by law to retain some or all of the Customer Personal Data. If you instruct us to delete Customer Personal Data, Customer Personal Data archived on our back up systems will be protected from further processing, and deleted when the required retention period has passed.

12. Customer Affiliate Communication and Rights. The entering into this DPA in the name and on behalf of a Customer Affiliate as set out in Section 1.2 constitutes a separate DPA between us and that Customer Affiliate, subject to the following:

12.1. Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with us under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Customer Affiliates.

12.2 Rights of Customer Affiliates. Where a Customer Affiliate becomes a party to the DPA with us, it shall to the extent required under Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

(i) Unless Data Protection Laws require the Customer Affiliate to exercise a right or seek a remedy under this DPA against MessageBird directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Customer Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Customer Affiliate individually but in a combined manner for itself and all of its Customer Affiliates together.

(ii) The parties agree that the Customer that is the contracting party to the Agreement shall, when an on-site audit of the procedures relevant to the protection of Customer Personal Data is being carried out on its behalf as set forth in Section 10.3 of this DPA, take all reasonable measures to limit any impact on us by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Customer Affiliates in one single audit.

For clarity, a Customer Affiliate does not become a contracting party to the Agreement.

13. California Consumer Privacy Act.

To the extent it is applicable, we make the following additional commitments to you with respect to processing of Customer Personal Data within the scope of the CCPA.

13.1 Our Obligations Under U.S. Data Protection Laws. The terms "business purpose," "commercial purpose," "consumer," "sell," and "share" as used in this Section 13.1 have the meanings given to them in the CCPA. Insofar as applicable, we shall comply with the CCPA and treat all Customer Personal Data subject to the CCPA and other applicable U.S. Data Protection Laws ("**U.S. Personal Data**") in accordance with the provisions of the CCPA and other U.S. Data Protection Laws. With respect to U.S. Personal Data, we are a service provider under the CCPA and a data processor under other U.S. Data Protection Laws. We shall not sell U.S. Personal Data. We shall not retain, use or disclose any U.S. Personal Data (i) for any purpose other than the business purposes specified in the Agreement (including retaining, using or disclosing U.S. Personal Data for a commercial purpose other than the business purpose specified in the Agreement or as otherwise permitted by the CCPA or applicable laws); or (ii) outside the direct business relationship with you and us.

13.2 Customer Obligations. You represent and warrant that you have provided notice to the End-User that the Personal Data is being used or shared in accordance with applicable Data Protection Laws. You are responsible for compliance with the requirements of the Data Protection Laws to the extent applicable to you as a data controller.

14. Governing Law and Dispute Resolution. Any dispute, claim, or controversy ("Disputes") arising out of or related to this DPA shall be governed by and construed in accordance with the laws of the Netherlands. Each Party agrees that the competent courts of Amsterdam will have exclusive jurisdiction to settle any Disputes arising out of or related to this DPA.

APPENDIX I - DETAILS OF PROCESSING

Where applicable, this Appendix I will serve as Annex I to the EEA Standard Contractual Clauses.

Annex I, Part A. List of Parties

Data exporter: Customer
Data exporter contact details: The address listed in Customer's account, or Customer's account owner email address, or to the email address(es) for which Customer elects to receive notices under the Agreement.
Data exporter role: The data exporter's role is outlined in Section 4 of the DPA.
Signature and date: If and when applicable, data exporter is deemed to have signed the Standard Contractual Clauses incorporated herein as of the Effective Date of the DPA.

Data importer: MessageBird
Data importer contact details: Data Protection Officer - privacy@messagebird.com
Data importer role: The data importer acts as data processor.
Signature and date: If and when applicable, data importer is deemed to have signed the Standard Contractual Clauses incorporated herein as of the Effective Date of the DPA.

Annex I, Part B. Description of Transfer

1. Categories of data subjects whose Personal Data is transferred.

- Users. Contact persons (natural persons) or employees, contractors or temporary workers (current, prospective, former) of Customer using the Services ("**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 over our communication platform.

2. Categories of Personal Data transferred.
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 personalised 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 communication such as voice call, SMS or email, whether it relates to an individual or a company.
- End-User data, such as phone number, email address, first name, last name, profile name, country, channel identifier.
- 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.

3. Sensitive data transferred. (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for personnel having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

(a) Communication content. 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, in accordance with Section 3.2 of the Agreement.

(b) Traffic data, End-User data, and customer usage data. No sensitive data is contained in traffic data, End-User data, or customer usage data.

4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Customer Personal Data is transferred on a continuous basis for the duration of the Agreement.

5. Nature of the processing: We will process Customer Personal Data to the extent necessary to provide the Services under the Agreement. We do not sell any Personal Data, including Customer Personal Data, and do not share Personal Data with third parties for compensation or for those third parties' own business interests.

6. Purpose(s) of the data transfer and further processing: We will process Customer Personal Data as a data processor in accordance with instructions of Customer as set forth in this DPA, unless processing is necessary for compliance with a legal obligation to which we are subject, in which case we will classify as a data controller.

Communication content, traffic data, **End-User data, and customer usage data.** Personal Data contained in communication content, traffic data, End-User data, and customer usage data will be subject to the following basic processing activities:

(a) Communication content. The provision of programmable communication products and services, offered in the form of application programming interfaces (APIs) or via the Dashboard, to Customer, including transmittal to or from Customer's software application from or to our communication platform, and other communications networks.

(b) Traffic data. Traffic data is processed for the purpose of transmitting communication on an electronic communications network or for the billing in respect of that communication. This may include Customer Personal Data about the routing, duration or timing of a communication such as voice call, SMS or email, whether it relates to an individual or a company.

(c) End-User data. Personal Data of End-Users is required in order to perform the Services and will only be processed for the purposes of communication transmission, customer support, and ensuring compliance with legal obligations of MessageBird.

(d) Customer usage data. Personal Data contained in customer usage data will be subject to the processing activities of providing the Services under the Agreement, with the aim of providing Customer with Services related insights and analytic reports regarding the communication sent, customer support, and continuous improvement of the Services.

7. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

(a) Communication content and traffic data.

- For communication content and traffic data contained in the SMS and Voice Services a retention period of six months applies;
- For Video Services communication content and traffic data are retained for a minimum of 30 days up to the duration as agreed upon with you;
- For Email services communication content and traffic data are retained for 72 hours;
- For all other services, communication content and traffic data are retained for the duration of the Services, except if you delete communication content or traffic data via the technical and organisational measures provided to you via the Services.

(b) End-User data. End-User data will be processed for the duration determined by the Customer,

when End-User data is included in your contact profiles the default retention period is for the duration of the Services, subject to Section 6(c) of this Annex I, Part B.

(c) Customer usage data. Upon termination of the Agreement, we may retain, use, and disclose Customer Usage Data for the purposes set forth in Section 6(d) of this Annex I, Part B, subject to the confidentiality obligations set forth in the Agreement. We will anonymize or delete customer usage data when we no longer require it for the purposes set forth in Section 6(d) of this Annex I, Part B.

8. For transfers to (Sub-)processors, also specify subject matter, nature and duration of the processing: For transfers to Sub-processors, the subject matter and nature of the processing is outlined at MessageBird's overview of Processors and Subprocessors and the duration is for the duration of the Agreement.

Annex I, Part C. Competent Supervisory Authority

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) will be the competent supervisory authority.

APPENDIX II - TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Where applicable, this Appendix II will serve as Annex II to the Standard Contractual Clauses. The following provides more information regarding our technical and organisational security measures set forth below.

Technical and Organisational Security Measures:

Measures of pseudonymization and protection of Personal Data in storage and transit: all Personal Data is encrypted in transit and at rest, and, to the extent relevant from a security standpoint, treated as if it were classified as sensitive data. Information is always transmitted over TLS with up-to-date encryption methodologies by default.

Measures for ensuring ongoing confidentiality, integrity, and availability and resilience of processing systems and services: we enter into agreements that contain confidentiality provisions with our employees, contractors, vendors, and Sub-processors. Our business continuity policy is to prepare our business and services in the event of extended outages caused by factors beyond our control and to restore services to the widest extent possible in a minimum time frame. We understand the services we provide are mission critical to our customers and therefore have very little tolerance for service disruptions. Our timeframes for recovery are designed to ensure we can meet our obligations to all of our customers

Processes for regular testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of processing: the goal of information security and our Information Security Management System (ISMS) is to protect the confidentiality, integrity and availability of information to the organisation, employees, partners, customers and the (authorised) information systems, and to minimise the risk of damage occurring by preventing security incidents and managing security threats and vulnerabilities. Our Legal team, Data Protection Officer, and Security Team make sure that applicable regulations and standards are factored into our security frameworks.

Measures for user identification and authorization: we follow principles of “need to know“ and “least privilege”. We promote the use of role based access control. Provisioning and deprovisioning is overseen by the security team, with Single-Sign-On and 2FA by default. Owners have been defined for each information asset who are responsible for ensuring access to their systems are appropriate and reviewed on a regular basis. Whenever dealing with sensitive information or taking critical action, we use the four-eyes principle.

Measures for ensuring events logging: audit logs are centrally stored and monitored on a regular basis for security events and are kept secure to avoid risk of tampering. The Incident Management Policy enforces the incident response plan and its procedures. These guidelines are being followed if any type of security or technical incident occurs.

Measures for ensuring systems configuration, including default configuration: we follow a consistent change management process for all the changes to the production environment of the Communication Platform as a Service. To elaborate further, all requests for changes (RFC) need to be approved by a designated party and executed according to the formal change control process. The control process ensures that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored. Configuration baselines are followed to securely configure the systems by following best-practices. Also, within the Engineering department, a tech radar is used to define which technologies (languages, platform tools, databases and data management tools) can be adopted or need to be avoided during development.

Measures for physical security: we actively promote a “Work from Anywhere” policy so our employees

are free to work from any place they want. However, we still have our office premises. We have no secure areas/data centre on our premises as we are a completely cloud-based company. Our office floors are protected by physical access controls, CCTV, and manned security.

Measures for internal IT and IT security governance and management: we maintain a risk-based assessment security program, which includes administrative, organisational, technical, and physical safeguards designed to protect the Services and confidentiality, integrity, and availability of Customer Data. Our information security program is set up in a systematic and well organised way. In addition, legal and regulatory requirements apply to ensure the confidentiality, integrity, and availability of information to the organisation, employees, partners and customers. All these are translated into our information security policies, procedures and guidelines. We have a Security Steering Committee which is responsible for the tactical level of information security. This entails the coordination of information security activities and the translation of strategic activities to operational activities for our security, and our continuous maintenance of regulatory compliance. All employees are responsible for safeguarding company assets. All our employees are screened for expertise, experience, and integrity. Employees are informed about security and data protection at the on-boarding stage, as well as by way of regular team-specific training, and other company-wide all-hands presentations about the importance of data protection and security compliance. MessageBird is ISO/IEC 27001:2013 certified, the globally recognised information security standards for Information Security Management Systems (ISMS).

- All our hosting providers are ISO/IEC 27001:2013 compliant.
- We are also registered with the Dutch Authority for Consumers and Markets. This means we're always accountable and fully transparent with our clients.
- We are an Associate Member of the Groupe Speciale Mobile Association (GSMA). The GSMA represents the interests of mobile operators across the globe.
- We are always up to the date with all applicable laws and regulations, including the General Data Protection Regulation.

Measures for certifications/assurance of processes and products: we undergo rigorous surveillance as well as certification audits as part of our ISO/IEC 27001:2013 compliance, and regularly execute application vulnerability and penetration testing.

Measures for ensuring accountability: we implement information security and data protection policies in accordance with applicable laws and publish an overview of our ISMS relevant information (link). We have appointed a dedicated Head of Information Security and a Data Protection Officer, and maintain documentation of our processing activities, including recording and reporting security incidents involving Personal Data where applicable.

Measures for ensuring data erasure: we ensure data erasure through an automated deletion process within our communication and infrastructure environment. This data deletion process ensures that all data that are no longer needed to fulfil a specific purpose are removed from our systems after processing.