Data Protection Addendum

This Data Protection Addendum ("Addendum") is entered into as of the date of the last signature below, (the "Effective Date"), by and between Doppler Technologies, Inc., a California corporation with its primary place of business at 340 S. Lemon Avenue #5880 Walnut, CA 91789 ("Doppler"), and the customer using Doppler's platform ("Customer") pursuant to the Doppler Terms of Service available at https://doppler.com/legal/terms, as updated from time to time, or other agreement between Customer and Doppler governing Customer's use of the Services (the "Agreement").

This Addendum is incorporated into and forms part of the Agreement. The terms used in this Addendum have the meaning set forth in this Addendum. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. The term of this Addendum shall follow the term of the Agreement. Except as modified below, the Agreement remains in full force and effect.

HOW TO EXECUTE THIS ADDENDUM

1. This Addendum consists of two parts: (i) the main body of the Addendum and (ii) Appendixes A and B
2. This Addendum has been pre-signed on behalf of Doppler.
3. To complete this Addendum, Customer must:
    a. complete the information in the signature box and sign on Page 9.
    b. Send the signed Addendum to Doppler by email to privacy@doppler.com.
4. Upon mutual execution of the Addendum by Doppler and Customer, this Addendum will become legally binding.

For the avoidance of doubt, executing this Addendum shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices.

HOW THIS ADDENDUM APPLIES

Doppler provides services to Customer under the Agreement. Pursuant to the Agreement, Doppler may from time to time process Personal Data (as defined below) for which Customer may be a "Data Controller" as defined by applicable privacy laws, including the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR").

Because such processing may, from time to time, require the maintenance and implementation of appropriate technical and organizational safeguards, and because such processing may, from time to time, involve the transfer of Personal Data from the European Union to the United States, Customer and Doppler have agreed to execute this Addendum in order to ensure that adequate safeguards are established with respect to the protection of Personal Data.

1. <u>Definitions</u>:

1. **“Affiliate”** means an entity that direct or indirectly Controls, or is Controlled by or is under common Control with an entity.

2. **“Agreement”** means Doppler’s Terms of Service or other written or electronic agreement, which govern the provision of the Service to Customer as such terms or agreement may be updated from time to time.

3. **"Applicable Data Protection Law"** shall mean all laws and regulations applicable to the processing of personal data under the Agreement. For the sake of clarity, Applicable Data Protection Law includes, without limitation 1) data protection laws and regulations of the European Union, the European Economic Area and their member states and Switzerland; and 2) data protection laws and regulations of the United Kingdom; 3) the California Consumer Privacy Act (“CCPA”); 4) the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”); and the Brazilian General Data Protection Law (“LGPD”), Federal Law no. 13,709/2018.

4. **“Control”** means an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term “Controlled” shall be construed accordingly.

5. **“Controller"** (controller includes “**Business**” as defined by the CCPA)**, "processor" (**processor includes “**Service Provider**” as defined by the CCPA)**, "data subject" (**data subject includes “**Consumer**” as defined by the CCPA)**, “personal data” (**personal data includes **“Personal Information”** as defined by the CCPA**)** and **"processing"** (and **"process"**) shall have the meanings given in Applicable Data Protection Law;

6. **“Customer”** shall mean the Customer entities or affiliates that are party to the Agreement.

7. **“Customer Information”** means any personal data that Doppler processes on behalf of Customer via the Service, as more particularly described in this Addendum.

8. **“EU Data Protection Law”** means all data protection laws and regulations applicable to Europe, including (i) 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 (“GDPR”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the

electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iii) in respect of the United Kingdom ("UK") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union.

9. **"Europe"** means, for the purposes of this Addendum, the European Union, the European Economic Area, and/or their member states, Switzerland, and the United Kingdom.

10. **"Doppler Services"** shall mean the services Doppler is providing pursuant to the Agreement.

11. **"Privacy Shield"** shall mean the EU-US and/or Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.

12. **"SCCs"** mean the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

13. **"Security Incident"** means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Information on systems managed or otherwise controlled by Doppler.

14. **"Service Data"** means any data relating to the Customer's use, support, and/or operation of the Service.

15. **"Sub-processor"** means any processor engaged by Doppler or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this Addendum. Sub-processors may include third parties or Affiliates of Doppler, but shall exclude Doppler's employees or consultants.

2. <u>Processing of Personal Data</u>:

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the processing of Customer Information, Customer is the data Controller and Doppler is the data Processor as further described in Appendix A (Details of Data Processing) of this Addendum. Each party shall comply with its obligations under Applicable Data Protection Law, and this Addendum, when processing Customer Information.

2.2 Customer Instructions. The parties agree that the Agreement, including this Addendum constitute Customer's complete and final instructions to Doppler in relation to the processing of Customer Information. Doppler shall process Customer Information only in

accordance with these instructions, as necessary to comply with applicable law, or as otherwise agreed in writing ("Permitted Purposes").

2.3 Customer Obligations. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Applicable Data Protection Law, in respect of its processing of Customer Information and any processing instructions it issues to Doppler; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Applicable Data Protection Law for Doppler to process Customer Information for the purposes described in the Agreement. Customer shall have the sole responsibility for the accuracy, quality, and legality of Customer Information and the means by which Customer acquired Customer Information. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Applicable Data Protection Law) applicable to any content created, sent, or managed through the Service.

2.4 Violations of Applicable Data Protection Law. Customer will ensure that Doppler's processing of the Customer Information in accordance with Customer's instructions will not cause Doppler to violate any applicable law, regulation, or rule, including without limitation Applicable Data Protection Law. Doppler will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate Applicable Data Protection Law.

2.5 Confidentiality Obligations of Doppler Personnel. Doppler will ensure that any person it authorizes to process the Customer Information shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

2.6 Return or Deletion of Customer Information. Upon Customer's request or upon termination of the Agreement, Doppler agrees, at Customer's option, to either deliver to Customer or destroy in a manner that prevents Customer Personal Data from being reconstructed, any Customer Personal Data and any copies in Doppler's control or possession, except that this requirement shall not apply to the extent Doppler is required by applicable law to retain some or all of the Customer Information or to Customer Information it has archived on back-up systems, which Customer Information Doppler shall securely isolate, protect from any further processing, and eventually delete in accordance with Doppler's deletion policies, except to the extent required by applicable law.

2.7 No Sale of Information. Doppler will not sell Customer Information, nor retain, use, or disclose Customer Information for any commercial purpose other than providing the Doppler Services. Doppler will not disclose Customer Information outside the scope of the Agreement. Doppler understands its obligations under Applicable Data Protection Law and will comply with them.

3. Rights of Data Subjects:

3.1 Data Subject Rights. To the extent Customer, in its ordinary use of the Doppler Services, does not have the ability to address a data subject request to exercise their rights under Applicable Data Protection Law, Doppler shall, upon Customer's request, provide commercially reasonable assistance to Customer in responding to such data subject request.

3.2 Responding to Requests. In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory or third party, including, but not limited to law enforcement, is made directly to Doppler in connection with Doppler's processing of Customer Information, Doppler shall promptly inform Customer providing details of the same, to the extent legally permitted. Unless legally obligated to do so, Doppler shall not respond to any such request, inquiry or complaint without Customer's prior consent. In the case of a legal demand for disclosure of Customer Information in the form of a subpoena, search warrant, court order or other compulsory disclosure request, Doppler shall attempt to redirect the requesting party or agency to request disclosure from Customer. Customer agrees that Doppler may provide Customer's basic contact information for this purpose. If Doppler is legally compelled to respond to such a request, Doppler shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy, unless Doppler is legally prohibited from doing so. For the avoidance of doubt, nothing in this Agreement, including this Addendum shall restrict or prevent Doppler from responding to any data subject or data protection authority requests in relation to personal data for which Doppler is a controller.

3.3 Data Protection Impact Assessments. If Doppler believes or becomes aware that its processing of Customer Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, Doppler shall inform Customer and (taking into account the nature of the processing and the information available to Doppler) provide reasonable cooperation to Customer in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law. Doppler shall comply with the foregoing by: (i) complying with Section 4.5 (Audits); (ii) providing the information contained in the Agreement, including this Addendum; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance at Customer's expense.

4. Security:

4.1 Technical and Organizational Measures. Doppler has implemented and will maintain appropriate technical and organizational security measures to protect Customer Information from Security Incidents and designed to preserve the security and

confidentiality of Customer Information in accordance with Doppler's security standards described in Appendix B ("Security Measures").

4.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by Doppler relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Applicable Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Doppler may update or modify the Security measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Service provided to Customer.

4.3 Security Incident Response. Doppler shall, to the extent permitted by law, notify Customer without undue delay of any reasonably suspected or actual Security Incident which affects Customer Information. The notice shall summarize in reasonable detail the nature and scope of the Security Incident, to the extent known, and the corrective action already taken or to be taken by Doppler. Furthermore, Doppler shall provide timely information relating to the Security Incident as it becomes known or as reasonably requested by Customer and promptly take reasonable steps to remedy or mitigate the effect of any Security Incident. Doppler's notification of or response to a Security Incident shall not be construed as an acknowledgement by Doppler of any fault or liability with respect to the Security Incident. The parties will collaborate on whether any notice of breach is required to be given to any person, and if so, the content of that notice. Unless prohibited by an applicable statute or court order, Doppler shall also notify Customer of any third-party legal process relating to any Security Incident, including, but not limited to, any legal process initiated by any governmental entity. Customer agrees that an unsuccessful Security Incident will not be subject to this Section 4.3 (Security Incident Response). An unsuccessful Security Incident is one that results in no unauthorized access to Customer Information or to any of Doppler's equipment or facilities used to store or process Customer Information.

4.4 Customer Responsibilities. Notwithstanding the above, Customer agrees that except as provided in this Addendum, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Information when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Information uploaded to the Service.

4.5 Audits. Subject to reasonable notice, Doppler shall provide Customer an opportunity, at Customer's cost and expense, to conduct a privacy and security audit of Doppler's security program and systems and procedures that are applicable to the services provided by Doppler to Customer. Audits will occur at most annually or following notice of a Security Incident and will be completed in no more than thirty (30) calendar days. If the audit

reveals any material vulnerability, Doppler shall take commercially reasonable steps to correct such vulnerability.

5. <u>Subcontracting</u>:

5.1 Authorized Sub-processors. Customer agrees that Doppler may engage third party sub-processors to fulfill its contractual obligations under this Addendum or to provide certain services on its behalf. The sub-processors Doppler currently engages to carry out processing activities can be found here. At least 10 days prior to engaging or removing any sub-processor, Doppler will update this list and provide Customer with a mechanism to obtain notice of that update. Customer may object to in writing to Doppler's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach resolution, Doppler will, in its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the Agreement without liability to either party.

5.2 **Sub-processor obligations.** Doppler shall: (i) conduct appropriate due diligence on each Sub-processor it engages to perform services on its behalf; (ii) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Information as those in this Addendum, to the extent applicable to the nature of the service provided by such Sub-processor; and (iii) remain responsible for such Sub-processor's compliance with the obligations of this Addendum and for any acts or omissions of such Sub-processor that cause Doppler to breach any of its obligations under this Agreement.

6. <u>International Transfers of Customer Personal Data</u>:

6.1 Data Center Locations. Customer agrees that Doppler may transfer and process Customer Information to and in the United States and any other country where Doppler or its Affiliates or Sub-processors conduct operations. Doppler shall ensure that such transfers comply with the requirements of Applicable Data Protection Laws.

6.2 European Data Transfers. To the extent that Doppler receives Customer Information protected by EU Data Protection Laws, Doppler agrees to abide by and process such data in compliance with the SCCs, which are incorporated in fully by reference and form an integral part of this Addendum. For the purposes of the SCCs: (i) Doppler is the "data importer" and Customer is the "data exporter" under the SCCs (notwithstanding that Customer may be an entity located outside the EU); and (ii) Appendixes A and B of this Addendum shall replace Appendixes 1 and 2 of the SCCs, respectively. For the avoidance of doubt, the SCCs will apply to Personal Data processed by Doppler in the context of providing the Services to Customer that are transferred from Europe to outside Europe, either directly or via onward

transfer, to (i) the United States when the transfer is not covered by a valid Privacy Shield certification, or (ii) any country or recipient not recognized by the European Commission as providing an adequate level of protection under EU Data Protection Law.

7. Limitation of Liability:

7.1 Liability Cap. Each party and all of its affiliates' liability taken together arising out of or related this this Addendum, including the SCCs, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

7.2. Liability to Data Subjects. Each Party agrees that it will be liable to Data Subjects for the entire damage resulting from a violation of Applicable Data Protection Laws. If one Party paid full compensation for the damage suffered, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's part of the responsibility for the damage. For that purpose, both Parties agree that Customer will be liable to Data Subjects for the entire damage resulting from a violation of EU Data Protection Law with regard to Processing of Personal Data for which it is a Controller, and that Doppler will only be liable to Data Subjects for the entire damage resulting from a violation of the obligations of EU Data Protection Law directed to Processor where it has acted outside of or contrary to Customer's lawful instructions. Doppler will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

8. Modification and Termination of this Addendum: This Addendum shall remain in effect for so long as Doppler processes Customer Information on behalf of Customer or until termination of the Agreement. Failure to comply with any of the material provisions of this Addendum is considered a material breach of the Agreement. In the event of termination, Doppler will return or destroy data pursuant to Section 2.7 (Return or Deletion of Customer Information). This Addendum may only be modified by a written amendment signed by each of the parties.

9. Entire Agreement; Conflict: This Addendum supersedes and replaces all prior and contemporaneous agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Customer and Doppler. If there is any conflict between this Addendum and any agreement, including the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) SCCs; then (b) this Addendum; then (c) the Agreement.

10. Service Data: Notwithstanding anything to the contrary in the Agreement (including this Addendum), Doppler shall have a right to collect, use, and disclose Service Data for its legitimate business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, develop, optimize, and maintain the Service; (iii) to investigate

fraud, spam, wrongful or unlawful use of the Service; and/or (iv) as required by applicable law. To the extent such Service Data is considered personal data under Applicable Data Protection Law, Doppler shall be responsible for and shall process such data in accordance with the Doppler Privacy Policy and Applicable Data Protection Laws. For the avoidance of doubt, this Addendum shall not apply to Service Data.

11. **Invalidity and Severability.** If any provision of this Addendum is found by any court or administrative body of competent jurisdiction to be invalid and unenforceable, the invalidity or un-enforceability of such provision shall not affect any other provision of this Addendum and all provisions not affected by such invalidity or un-enforceability will remain in full force and effect.

IN WITNESS WHEREOF, the Parties acknowledge their agreement to the foregoing by due execution of the Addendum by their respective authorized representatives.

CUSTOMER	**DOPPLER, INC.**
Signature: _____	Signature:_____
Customer Legal Name: _____	Print Name: _____
Print Name: _____	Title: _____
Title: _____	
Date: _____	Date:_____
DPO/Contact for data protection enquiries: _____ _____	DPO/Contact for data protection enquiries: Privacy Team privacy@doppler.com

Appendix A – Details of Processing

Subject matter:

The subject matter of the data processing under this Addendum is the Customer Information.

Duration of the processing:

Doppler will process Customer Information as outlined in Section 2.2 (Customer Instructions), 2.7 (Return or Deletion of Customer Information), and 8 (Modification and Termination of this Addendum) of this Addendum.

Purpose:

Doppler shall only process Customer Information for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of the Agreement.

Categories of data subjects:

Customer may submit personal data in course of using Doppler's services, the extent of which is determined and controlled by Customer in its sole discretion and may include, but is not limited to personal data relating to Customer, Customer's contacts, and Customer's authorized users, which includes Customer's employees and contractors who are granted per-user access rights to Doppler's Services.

Types of Customer Information:

Customer may upload, submit, or otherwise provide certain personal data to the Service, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data:

- Full name and contact information
- Company name and job title
- Billing and payment information
- Any other personal data submitted by, sent to, or received by Customer or Customer's authorized users via the Doppler Services.

Special categories of data:

The parties do not anticipate the transfer of special categories of data.

Processing Operations:

Customer Information will be processed in accordance with the Agreement (including this Addendum) and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain, and improve the service provided to Customer pursuant to the Agreement; and/or

- Disclosure in accordance with the Agreement and/or as compelled by applicable law.

Appendix B – Security Measures

Doppler will, at a minimum, implement the following types of security measures:

1. Virtual Access Control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (e.g., minimum length and multifactor authentication features);
- Automatic blocking (e.g. password or timeout); and
- Encryption of archived data media.

2. Data Access Control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Customer Information in accordance with their access rights, and that Customer Information cannot be read, copied, modified, or deleted without authorization include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions, and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Customer Information without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure; and
- Encryption.

3. Disclosure control

Technical and organizational measures to ensure that Customer Information cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Customer Information is disclosed, include:

- Encryption/tunneling;
- Tokenization;

- Logging; and
- Transport security.

4. Entry Control

Technical and organizational measures to monitor whether Customer data have been entered, changed, or removed, and by whom, from data processing systems, include:

- Logging and reporting systems.

5. Control of Instructions

Technical and organizational measures to ensure that Customer Data are processed solely in accordance with the instructions of the Controller include:

- Clear contract phrasing.

6. Availability Control

Technical and organizational measures to ensure that Customer Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Redundant storage; and
- Remote storage.

7. Separation Control

Technical and organizational measures to ensure that Customer Data collected for different purposes can be processed separately include:

- Separation of databases;
- Segregation of functions (production/testing); and
- Procedures for storage, amendment, deletion, transmission of data for different purposes.