Data Processing Addendum

This Data Processing Addendum ("**Addendum**") forms part of the Subscription Agreement ("**Agreement**") between _____ ("**Customer**") and Pipeline Signals, Inc. ("**Vendor**") under which Vendor provides services to Customer ("**Agreement**"). Customer and Vendor are referred to herein as "**Parties**" and individually as "**Party**".

1. **Definitions.**

   a. **"Controller"** means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For purposes of this Addendum, Customer is the Controller.
   b. **"Processor"** means the entity which Processes Personal Data on behalf of the Controller. For purposes of this Addendum, Vendor is the Processor.
   c. **"Data Protection Laws"** means all data protection laws applicable to the Processing of Personal Data under this Addendum, including local, state, national and/or foreign laws, treaties, and/or regulations, the California Consumer Privacy Act, the California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Personal Data Privacy and Online Monitoring Act, the Utah Consumer Privacy Act, and all regulations implementing the foregoing laws.
   d. **"Data Subject"** means the person to whom the personal Data relates.
   e. **"Personal Data"** means any data that is Processed by Vendor in connection with the Services that relates to (i) an identified or identifiable natural person or, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data under applicable Data Protection Laws).
   f. **"Security Breach"** means (i) a breach of security leading to the accidental, unlawful or unauthorized access, use, intrusion, or breach of security of Vendor IT systems; (ii) any destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data collected, transmitted, stored or otherwise Processed by Vendor; and (iii) any other adverse event that affects or may affect Vendor IT Systems or Customer IT systems.
   g. **"Processing or Process"** means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.
   h. **"Services"** are those products, services, and other deliverables provided under the Agreement.

The terms **Sell** and **Share** have the definitions provided under Data Protection Laws. Any other terms that are not defined herein shall have the meaning provided under the Agreement or under Data Protection Laws.

2. **Instructions for Processing and Compliance with Laws.**
   a. Vendor shall Process Personal Data for the sole purpose of providing Services under the Agreement and strictly in accordance with the Agreement and this Addendum. The Parties agree that Services will be conducted in accordance Attachment A of this Addendum, which describes the nature and purpose of the Processing, the type of personal data Processed, and the categories of Data Subjects. Vendor shall not Process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of Personal Data to any third party other than in accordance with Customer's documented instructions (whether in the Agreement, this Addendum or otherwise).
   b. Vendor represents and warrants that: (i) it is in compliance with Data Protection Laws; (ii) it shall Process Personal Data in compliance with Data Protection Laws; and (iii) it will not Process data in manner that will put Customer in violation of Data Protection Laws.
   c. Vendor represents and warrants that it will not Process, collect, or transfer the Personal Data of individuals residing outside the United States in its provision of Services to Customer.

d. Vendor agrees that to the extent it collects and Processes Personal Data on behalf of Customer, it is authorized to do so, and has obtained any necessary consent required by Data Protection Laws to Process Personal Data under the Agreement, and Vendor represents and warrants that it has all authorizations and consents required by Data Protection Laws to Process Personal Data.

3. **Vendor Processing Obligations.** Without limiting the generality of the foregoing, Vendor is prohibited from:
   a. Selling or Sharing Personal Data;
   b. Retaining, using, disclosing, or otherwise Processing Personal Data for any purpose other than for the specific purpose of providing Services under this Agreement, including but not limited to disclosing Personal Data for a commercial purpose other than providing Services specified in the Agreement;
   c. Retaining, using, disclosing, or otherwise Processing Personal Data outside of the direct business relationship between Customer and Vendor; and
   d. Combining Personal Data received from or on behalf of the Customer with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, except where both (i) expressly required to perform the Services and (ii) permitted by Data Protection Laws.
   e. Vendor shall, in performing the Services, ensure the security of Personal Data including by: (i) complying with Data Protection Laws; (ii) providing the same level of privacy protection as is required by Data Protection Laws to Personal Data; and (iii) ensuring each person Processing Personal Data (including but not limited to employees, agents, and subcontractors) is subject to a duty of confidentiality with respect to such Personal Data;
   f. Vendor shall allow Customer to take reasonable and appropriate steps to help ensure that Vendor uses Personal Data in a manner consistent with Customer's obligations under Data Protection Laws;
   g. Vendor shall notify Customer promptly in writing if it makes a determination that it can no longer meet its obligations under Data Protection Laws, reasonably specifying which obligations it has determined it can no longer meet;
   h. Vendor grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate Vendor's unauthorized use of Personal Data;
   i. Vendor shall allow and cooperate with reasonable assessments by Customer, or its designated assessor to conduct an assessment of Vendor's policies and technical and organizational measures in support of the obligations under Data Protection Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessments.
   j. Vendor shall adhere to the instructions of Customer and shall assist Customer in meeting its obligations under Data Protection Laws. Such assistance shall include:
      i. Helping to fulfill Customer's obligation to respond to Consumer rights requests under Data Protection Laws (provided, however, that if an individual makes any such request to Vendor, Vendor shall inform the individual that Vendor cannot respond to the request because it is a Processor); and
      ii. Deleting any Personal Data that Customer directs Vendor to delete as a result of an individual's request made to Customer pursuant to Data Protection Laws and shall notify any of its own service providers or subcontractors to delete such Personal Data to the extent collected, used, Processed, or retained by the service provider or subcontractor.
   k. Vendor hereby certifies that it understands the restrictions set forth in this Section and will comply with them.

4. **Subcontractors.** Vendor may utilize agents and subcontractors to perform the Services, provided that (i) Vendor provides Customer a reasonable opportunity to object to the engagement of such agent or subcontractor, (ii) such agents and subcontractors agree in writing to be bound by the same terms and conditions that apply to Vendor through this Addendum, (iii) Vendor conducts reasonable due diligence to ensure such agents or subcontractors are able to comply with the requirements herein and Vendor remains responsible and liable for any acts or omissions

of such agents and subcontractors, and (iv) Vendor agrees to provide a list of such agents or subcontractors to Customer upon request.

5. **Security.** Vendor shall implement appropriate technical and organizational measures designed to protect Personal Data against unauthorized access or disclosure or accidental or unlawful destruction, loss, or alteration. Such measures shall be appropriate to (i) the size, scope, and type of Vendor's business; (ii) the type of information that Vendor will Process; and (iii) the need for security and confidentiality of such information.

6. **Breach Notification.** Vendor shall promptly (and in any case not more than twenty-four (24) hours after becoming aware of a Security Breach) notify Customer of any Security Breach. The notice will include, at a minimum, subject to the availability of necessary information, the following: (i) the date or date range of the Security Breach; (ii) the date the Vendor discovered the Security Breach; (iii) a description of the Security Breach; (iv) the number of Data Subjects affected by the Security Breach; (v) types of Personal Data involved in the Security Breach; the likely consequences of the Security Breach; and the steps that Vendor has taken to investigate the Security Breach, mitigate potential harm and possible adverse effects, and prevent further Security Breaches; and (vi) the contact information for Vendor's data protection officer, if any, or such other person responsible for Vendor's response to the Security Breach. Vendor will promptly supplement the notice as necessary with information about the Security Breach as Vendor obtains the information, including Vendor's assessment as to whether the Security Breach is reportable under Data Protection Laws. All reports required by this provision shall be made to Customer's Group General Counsel at natasha.davidson@Customer.com. Vendor acknowledges its determination that a particular set of facts constitutes a Security Breach and its assessment whether the Security Breach must be reported is not binding on Customer. Vendor shall fully cooperate in the investigation of the Security Breach and provide sufficient information to allow Customer to meet its obligations under Data Protection Laws or under contract, if applicable. To the extent that Customer is subject to or involved in an investigation by a governmental authority, litigation, or any inquiry, formal or informal, arising out of or related to a Security Breach, Vendor will provide full cooperation to Customer in responding to such event. To the extent any applicable law requires that the affected Data Subjects or governmental authority be notified of a Security Breach, Vendor will be responsible for, at its own cost and expense, and indemnify Customer for:
   a. At Customer's request, and where possible under law, providing such notices to Data Subjects or governmental authorities containing the information required by applicable law, and Vendor will obtain Customer's prior approval of any content, form and timing of such notice;
   b. Conducting any forensic and security review, investigation and audit in connection with such Security Breach;
   c. Providing remediation services and other reasonable assistance to such Data Subjects as (a) required under law, (b) requested by governmental authorities, or (c) as reasonably requested by Customer; and
   d. Providing full cooperation to Customer in responding to such Security Breach.

7. **Audit.** Vendor shall make available, upon reasonable request, information necessary to demonstrate compliance with this Addendum and shall allow for audits or inspection by Customer in relation to the Processing of Personal Data under the Agreement.

8. **Indemnification; Limitations on Liability; Remedies.** Vendor agrees to indemnify and hold harmless Customer against all claims or threats of claims, cost, losses, liabilities, expenses (including attorneys' fees) and regulatory or similar actions or investigations (including any and all fines, fees, penalties, and assessments of any nature or kind imposed on or affecting, directly or indirectly, Customer) resulting from, arising out of or relating to (i) Vendor's breach of this Addendum; (ii) any Processing of Personal Data in violation of this Addendum; (iii) any Security Breach involving Personal Data in the possession, custody or control of Vendor or its subcontractors; (iv) any other breach of this Addendum by Vendor; (v) any claim or other action

filed against Customer related to Vendor's infringement of a privacy right. Any limitation of liability provided in the Agreement shall not apply to this Addendum.

9. **Deletion of Personal Data.** Upon termination of the Services, Vendor shall, at Customer's option, and to the extent applicable to the Services under the Agreement, permanently and securely delete all Personal Data collected on behalf of Customer and permanently and securely delete existing copies and ensure that all subcontractors do the same, unless applicable law requires continued retention of the Personal Data. In such case, Vendor shall continue to ensure the confidentiality of all such Personal Data, and this Agreement shall continue to apply to all retained Personal Data for as long as it remains in the possession of Vendor or its subcontractors.

10. **General Provisions**
    a. **Termination.** The term of this Addendum will end simultaneously and automatically with the termination of the Agreement except to the extent Vendor or any of its subcontractors retains Personal Data pursuant to Section 9 subsequent to the termination of the Agreement.
    b. **Conflict.** In the event of a conflict between the provisions of this Addendum and the Agreement, the provisions of this Addendum will prevail with regard to the Parties' data protection obligations.
    c. **Section Headings.** The section headings contained in this Addendum are for reference purposes only and shall not in any way affect the meaning or interpretation of this Addendum.

Attachment A

Customer's instructions for processing Personal Data are:

As set forth in Section 2 of the Agreement.

The nature and purpose of Vendor's processing is:

As set forth in Section 3 of the Agreement.

The type of Personal Data subject to Processing by Vendor is:

From the Client, the following information is requested:

Section	Field	Mandatory or Optional	Objective/Notes
Account Owners	Name	Optional	This is the first and last name of the individual who "owns" this account, indicating overall revenue responsibility. These are usually Account Executives, Account Managers, Customer Success Managers, etc.
	Email	Optional	We need this individual's email to give them access to view and modify their account list and communicate as needed.
	CRM ID	Optional	Knowing this person's CRM ID allows us to pass data to you for easy upload.
Direct Leader	Name	Optional	This is the first and last name of the person who is the direct leader of the "account owner".
	Email	Optional	This is the direct leader's email address for communication and updates.
Signal Recipients	Name	Optional	This is the first and last name of the individual who will receive and **action the signals**. In some situations, one person may own the revenue responsibility of the account (such as an Account Executive) but they'll have support from SDRs or BDRs to help action data into appointments or meetings.
	Email	Optional	We need this individual's email to give them access to view and modify their account list and communicate as needed.
	CRM ID	Optional	Knowing this person's CRM ID allows us to pass data to you for easy upload.
Account Information	Account Name	Mandatory	This is the name of the organization or account you'd like us to monitor for signal intelligence.
	Account Type	Mandatory	This is a drop-down field. You must choose one of these options.
	CRM ID	Optional	Knowing this account's CRM ID allows us to pass data to you for easy upload.
Account Segmentation Details	Geography/Market	Optional	If you'd like for us to link signals to particular markets or geographies (as per your process or better reporting), please provide that information here.

	BU/Division	Optional	If you'd like for us to link signals to particular business units or divisions (as per your process or better reporting), please provide that information here.
	Team Name	Optional	If you'd like for us to link signals to particular team names (as per your process or better reporting), please provide that information here.

Note that all signals discovered for you are never shared with other parties and will not be used for Pipeline Signals for any other purpose.

Data provided by Pipeline Signals:

Once we process your data, Pipeline Signals will send you the following in each data record where a sales opportunity is possible:

- Name of the person
- LinkedIn URL of the person
- Work/corporate email address of the person
- Name of the organization where the person previously worked
- CRM ID code of the organization where the person previously worked
- Name of the organization where the person currently works
- CRM ID code of the organization where the person currently works

In addition, if the Client does provide us with any of the information requested, the data record will be appended with:

- Name of seller
- CRM ID code of seller
- Email address of seller

Customer:

Signature:

Full Name:

Title:

Vendor: Pipeline Signals Inc.

Signature: DocuSigned by: Jamie Shanks 77E0F5AB520142A...

Full Name: Jamie Shanks

Title: CEO