Pinecone BYOC is in public preview. Run Pinecone inside your AWS, GCP, or Azure account with a zero-access operating model. - Read the blog Dismiss

LEGAL

Data Processing Addendum

2024-05-24

This Data Processing Addendum, inclusive of the Standard Contractual Clauses where applicable (collectively, this "*DPA*"), forms a part of the Master Subscription Agreement or other written or electronic services or subscription agreement that references this DPA (as applicable, the "Agreement") between Pinecone Systems, Inc., a Delaware (USA) corporation ("*Pinecone*") and the customer for Pinecone's Services under the Agreement ("*Customer*"). All capitalized terms not defined in this DPA shall have the respective meanings assigned to them in the Agreement. Pinecone may modify this Agreement from time to time, subject to Section 15 below.

1. **Definitions.** All capitalized terms not defined in this DPA shall have the respective meanings assigned to them in the Agreement. Capitalized terms not otherwise defined in the Agreement or this DPA shall have the respective meanings assigned to them in this Section.
    - "*Authorized Affiliate*" means an Affiliate of Customer that is authorized by Customer to use Services under the Agreement and has not entered into its own separate agreement with Pinecone.
    - "*CCPA*" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("*CPRA*"), each as may be amended, superseded or replaced from time to time.
    - "*Customer Personal Data*" means Personal Information contained within Customer Data.

- "*Data Protection Laws*" means all data protection and privacy laws and regulations applicable to the respective Party in its role in the processing of Customer Personal Data under the Agreement, which may include, to the extent applicable, European Data Protection Laws and the CCPA, Colorado Privacy Act, Connecticut Personal Data Privacy and Online Monitoring Act, Utah Consumer Privacy Act, Virginia Consumer Data Protection Act, and other similar U.S. state laws.
- "*Data Subject Request*" means a request from a data subject exercising a right under Data Protection Laws that relates to Customer Personal Data.
- "*European Data Protection Laws*" means (a) the General Data Protection Regulation 2016/679 together with any national implementing laws ("*EU GDPR*"); (b) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("*UK GDPR*"); and (c) the Swiss Federal Act on Data Protection and its implementing regulations ("*Swiss FADP*"); in each case as may be amended, superseded or replaced from time to time.
- "*European Transfer*" means a transfer (directly or via onward transfer) of personal data that is subject to European Data Protection Laws to a third country outside the European Economic Area, United Kingdom and Switzerland which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).
- "*Party*" means each of Pinecone and Customer.
- "*Personal Information*" means information relating to an identified or identifiable natural person, and includes "personal information", "personal data", and "personally identifiable information" and similar terms as defined in Data Protection Laws.
- "*Security Incident*" means a breach of Pinecone's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
- "*Security Measures*" means Pinecone's Technical and Organizational Security Measures, made available at https://www.pinecone.io/legal/security-measures.pdf.
- "*Standard Contractual Clauses*" or "*SCCs*" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded or replaced from time to time.
- "*Subprocessor*" means a Pinecone Affiliate or third party engaged by Pinecone to process Customer Personal Data in connection with the provision of Services.
- "*Trust Center*" means the Pinecone Trust and Security Center at https://security.pinecone.io/.
- "*UK Addendum*" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioners Office under S.119 (a) of the UK Data

Protection Act 2018, as updated or amended from time to time.

- In addition, the terms "*controller*", "*data subject*", "*supervisory authority*", "*processor*", "*process*", and "*processing*" have the meanings given to them in Data Protection Laws. The term "*controller*" includes "*business*", the term "*data subject*" includes "*consumers*", and the term "*processor*" includes "*service provider*", in each latter case, as defined by the CCPA.

2. **Processing of Personal Data**.
   - 2.1 Scope and Roles. This DPA applies when Customer Personal Data is processed by Pinecone as a processor in its provision of Services to Customer, who will act as a controller or processor, as applicable, of Customer Personal Data.
   - 2.2 Pinecone Processing. The details of the processing of Customer Personal Data by Pinecone are outlined in Schedule 1 of this DPA. Pinecone agrees to comply with Data Protection Laws in its processing of Customer Personal Data. Pinecone will process Customer Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with Customer's documented instructions (as set forth in the Agreement, in this DPA, or as directed by Customer or End Users through use of Services). Pinecone is not responsible for determining if Customer's processing instructions are compliant with law, but agrees to notify Customer in writing in accordance with Data Protection Laws if, in Pinecone's reasonable opinion, Customer's processing instructions infringe Data Protection Laws.
   - 2.3 Customer Processing. Customer agrees to comply with Data Protection Laws in its processing of Customer Personal Data and all processing instructions it issues to Pinecone. Customer represents and agrees that (a) it has provided notice and obtained all consents and rights necessary under Data Protection Laws for Pinecone to process Customer Personal Data and provide Services pursuant to the Agreement, including this DPA and (b) it shall in no event include special categories of personal data (GDPR article 9), personal data relating to criminal convictions and offenses (GDPR article 10), or similarly sensitive personal data subject to Data Protection Laws in any Customer Data.
3. **Duration**. This DPA shall remain in full force and effect through expiration or earlier termination of the Agreement. Accordingly, this DPA will co-terminate with the Agreement.
4. **Security and Confidentiality**. Pinecone has implemented and will maintain the Security Measures. The Security Measures are subject to technical progress and development and Pinecone may modify the Security Measures from time to time, provided that any modifications do not materially diminish the overall security of Services used by Customer during the applicable Subscription Term. Pinecone shall ensure that all employees, agents, contractors and Subprocessors authorized to process Customer Data are subject to appropriate confidentiality obligations.

5. **Subprocessors.**
    5.1 Requirements. Pinecone shall enter into a written agreement with its Subprocessors which includes data protection and security measures no less protective than the measures set forth in this DPA. Pinecone remains fully liable for any breach of this DPA that is caused by an act, error or omission of its Subprocessors to the same extent that Pinecone would have been liable for such act, error or omission had it been caused by Pinecone.
    5.2 Authorization. Customer provides a general authorization to Pinecone's use of Subprocessors to process Customer Personal Data in accordance with this Section, including all Pinecone Affiliates and the third-party Subprocessors identified at https://www.pinecone.io/legal/subprocessors/ (the "*Subprocessor List*").
    5.3 Updates; Objections. Pinecone will update the Subprocessor List prior to authorizing new Subprocessor(s) to process Customer Personal Data. The Subprocessor List includes, or links to, a mechanism to subscribe for notifications of new Subprocessors (each, an "*Update Notice*"). Customer may object to Pinecone's appointment of a new Subprocessor on reasonable data protection grounds by notifying Pinecone in writing at privacy@pinecone.io within 15 days of an Update Notice (an "*Objection Notice*"). In such event, Pinecone and Customer will discuss those objections in good faith with a view to achieving resolution. If the Parties are unable to achieve resolution within 14 days of the applicable Objection Notice, Customer, as its sole and exclusive remedy, may terminate its Service subscriptions with respect to those aspects of Services which cannot be provided by Pinecone without the use of the new Subprocessor and Pinecone will refund to Customer any associated unused amounts prepaid by Customer.
6. **Assistance.**
    6.1 Data Subject Requests. Customer is responsible for responding to, and complying with, Data Subject Requests. To the extent Customer is unable through its use of Pinecone Services to address a particular Data Subject Request on its own, Pinecone will, taking into account the nature of the processing, provide reasonable assistance to Customer to enable Customer to respond to the Data Subject Request. If Pinecone receives a Data Subject Request directly, Pinecone will promptly forward such request to Customer and Pinecone shall not, unless legally compelled to do so, respond directly to the data subject except to refer them to the Customer to allow Customer to respond as appropriate.
    6.2 Data Protection Impact Assessments. Pinecone will provide reasonably requested information regarding Services to Customer to carry out data protection impact assessments relating to the processing of Customer Personal Data and any related required consultation with supervisory

authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

6.3 Legal Requests. If Pinecone receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Customer Personal Data, Pinecone will attempt to redirect the governmental body to request such Customer Personal Data directly from Customer. As part of this effort, Pinecone may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Personal Data to a governmental body, Pinecone will give Customer reasonable notice of the legal demand to allow Customer to seek a protective order or other appropriate remedy, unless Pinecone is legally prohibited from doing so.

7. **Security Incidents**.

7.1 Reporting. Pinecone will notify Customer in writing without undue delay, and in any event within any time period required by Data Protection Law, after becoming aware of a Security Incident. The notification will describe (a) the nature of the Security Incident; (b) the steps Pinecone has taken, and plans to take, to address the Security Incident; and (c) any steps Pinecone recommends that Customer take in relation to the Security Incident. If Pinecone is unable to provide all such information in its initial notification, Pinecone will provide the information to Customer on a rolling basis as it is available.

7.2 Response. Pinecone will promptly take reasonable steps to investigate, contain, remediate and mitigate adverse effects from any Security Incident.

7.3 Notices to Others. In the event of a Security Incident, Pinecone will reasonably cooperate with and assist Customer with respect to any required notification to supervisory authorities or data subjects (as applicable), taking into account the nature of the processing, the information available to Pinecone, and any restrictions on disclosing the information (such as confidentiality). Unless precluded by law, Customer will make reasonable efforts to provide Pinecone advance copies of any such notices and allow Pinecone an opportunity to provide corrections or clarifications.

7.4 Disclaimers. Pinecone's notification of, or response to, a Security Incident will not constitute an acknowledgment of fault or liability with respect thereto. Further, Pinecone's obligations in this Section 7 do not apply to any Security Incident caused by Customer, its Affiliates, their End Users or any Customer System.

8. **Audits**. Upon written request and at no additional cost to Customer, Pinecone shall provide Customer (directly or through an appropriately qualified third-party auditor subject to written confidentiality obligations (an "*Authorized Auditor*")) access to documentation evidencing Pinecone's compliance with its obligations under this DPA. Such evidence will be in the form of certifications or extracts from relevant audits made available through the Trust Center. If Pinecone's compliance with this

DPA cannot be demonstrated through information available through the Trust Center, to the extent required by Data Protection Law, Customer may request in writing to conduct an audit at Customer's expense of Pinecone's applicable controls. Any such audit shall subject to the following: (a) Pinecone and Customer must mutually agree on the details of the audit, including the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, the audit; (b) the results of the audit must be promptly disclosed to Pinecone; (c) the audit, results and all associated information shall be Confidential Information (as defined in the Agreement) and may only be shared with third parties (other than Authorized Auditors) with Pinecone's prior written consent; and (d) Customer may not perform more than one audit in any 12-month period, except where required by a competent supervisory authority.

9. **Retrieval and Deletion**. Upon expiration or termination of the Agreement, Customer may retrieve any Customer Personal Data it wishes to retain as described in the Agreement and, unless prohibited by Applicable Law, Pinecone will delete Customer Personal Data in accordance with the Documentation and Agreement.
10. **Locations**. Certain Services or Service features may allow Customer to select a particular Cloud Provider's geographic region for processing certain Customer Data (each, a "*Cloud Designation*"), for example, to mitigate latency in Customer's use of Services. Customer acknowledges that a Cloud Designation does not preclude Pinecone from using other Cloud Providers or Cloud Provider regions in connection with its provision of Services to Customer. Subject to Data Protection Laws and other Applicable Laws (e.g., export control), Customer acknowledges that Pinecone may process Customer Personal Data where Pinecone, its Affiliates or Subprocessors maintain data processing operations.
11. **Territory-Based Requirements**.
    - 11.1 California Service Provider. Without limiting its other obligations under this DPA, with respect to Customer Personal Data subject to the CCPA, Pinecone confirms that it will not: (a) process, retain, use, or disclose Customer Personal Data for any purpose other than for the purposes set out in the Agreement (including this DPA) and as permitted under the CCPA; (b) combine Customer Personal Data with Personal Information that Pinecone receives from others; (c) sell or share Customer Personal Data. The terms "*sell*" and "*share*" shall have the meanings given to them in the CCPA. Pinecone agrees to notify Customer if Pinecone determines that it cannot meet its obligations under the CCPA or CPRA.
    - 11.2 European Transfers. Where the transfer of Customer Personal Data to Pinecone is a European Transfer and Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses. The Standard Contractual Clauses are incorporated into this DPA as provided in Section 11.3 through 11.5 and form an integral part of the Agreement. In the event Pinecone adopts an alternative transfer mechanism following the effective date of this

DPA (e.g., the EU-U.S. Data Privacy Framework administered by the U.S. Department of Commerce), such alternative transfer mechanism shall apply instead of the Standard Contractual Clauses, but only to the extent such alternative transfer mechanism complies with applicable European Data Protection Laws and extends to the territories to which Customer Personal Data is transferred.

11.3 EU GDPR. In relation to transfers of Customer Personal Data protected by the EU GDPR, the SCCs apply as follows:

11.3.1 Module Two terms will apply where Customer is the controller of Customer Personal Data (and Pinecone is the processor) and the Module Three terms will apply where Customer is the processor of Customer Personal Data (and Pinecone is the subprocessor);

11.3.2 in Clause 7, the optional docking clause will apply and Authorized Affiliates may accede to the SCCs under the same terms and conditions as Customer upon the mutual agreement of the Parties;

11.3.3 in Clause 9, Option 2 will apply and the time period for prior notice of subprocessor changes shall be as set out in Section 5.1 of this DPA;

11.3.4 in Clause 11(a), the optional language will not apply;

11.3.5 in Clause 17, Option 1 will apply and the SCCs will be governed the laws of Ireland;

11.3.6 in Clause 18(b), disputes shall be resolved before the courts of Ireland;

11.3.7 Annex I shall be deemed completed with the information set out in Schedule 1 to this DPA;

11.3.8 Annex II shall be deemed completed with the information set out in Schedule 2 of this DPA; and

11.3.9 Annex III shall be deemed completed with the Subprocessor List.

11.4 UK GDPR. In relation to transfers of Customer Personal Data protected by the UK GDPR, the SCCs as implemented under Section 11.3 above shall apply with the following modifications:

11.4.1 the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this DPA;

11.4.2 Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Section 11.3 above and Schedules 1 and 2 of this DPA, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting “neither party”; and

11.4.3 Any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Sections 9 through 11 in Part 2 of the UK Addendum.

11.5 Swiss FADP. In relation to transfers of Customer Personal Data protected by the Swiss FADP, the SCCs as implemented under Section 11.3 above will apply with the following modifications:

11.5.1 references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss FADP and the equivalent articles or sections therein;

11.5.2 references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and/or "Swiss law" (as applicable);

11.5.3 references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland;

11.5.4 the SCCs shall be governed by the laws of Switzerland; and

11.5.5 disputes shall be resolved before the competent Swiss courts.

11.6 EU/UK/Swiss Interpretations. Where the Standard Contractual Clauses apply pursuant to Section 11.2 of this DPA, this Section sets out the Parties' interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a Party complies with the interpretations set out below, that Party shall be deemed by the other Party to have complied with its commitments under the Standard Contractual Clauses:

11.6.1 where Customer is itself a processor of Customer Personal Data acting on behalf of a third party controller and Pinecone would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), Pinecone may interact solely with Customer and Customer shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;

11.6.2 taking into account the nature of the processing Customer Data by Pinecone, Customer acknowledges it is unlikely Pinecone would become aware that Customer Personal Data is inaccurate or outdated, but to the extent Pinecone becomes aware of such inaccurate or outdated data, Pinecone will inform the Customer in accordance with Clause 8.4 of the SCCs;

11.6.3 for the purposes of Clause 15(1)(a) of the SCCs, Pinecone shall notify Customer and not the relevant data subject(s) in case of government access requests, and Customer shall be solely responsible for notifying the relevant data subjects as necessary; and

11.6.4 the certification of deletion described in Clause 16(d) of the SCCs shall be provided following Customer's written request.

12. **Authorized Affiliates**. Customer is entering into this DPA on behalf of itself and, if applicable and to the extent required under Data Protection Laws, Authorized Affiliates. For purposes of this DPA only, and except where otherwise indicated, the term "Customer" shall include both Customer and Authorized Affiliates. Accordingly, Pinecone' obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following: (a) Customer is solely responsible for communicating any additional processing instructions on behalf of its Authorized Affiliates; (b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations under this DPA; and (c) if an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Pinecone (an "*Affiliate Claim*"), Customer must bring such Affiliate Claim directly against Pinecone on behalf of the Authorized Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim, and all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability. In no event will this DPA or any Party restrict or limit the rights of any data subject or of any competent supervisory authority.
13. **Liability**. Notwithstanding anything to the contrary in the Agreement or this DPA and to the fullest extent permitted by law (including Data Protection Law), each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, the SCCs or any data protection agreements in connection with the Agreement (if any), whether in contract, tort or under any other theory of liability, shall remain subject to the limitation of liability provisions of the Agreement and any reference in such provisions to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and this DPA. Customer agrees that any regulatory penalties incurred by Pinecone that arise in connection with Customer's failure to comply with its obligations under this DPA or any laws or regulations including Data Protection Laws shall reduce Pinecone's liability under the Agreement as if such penalties were liabilities to Customer under the Agreement.
14. **General**.

14.1 Prior Terms. This DPA shall replace any existing data processing addendum, attachment, exhibit or standard contractual clauses that the Parties may have previously entered into in connection with Services.

14.2 Reimbursement. To the fullest extent permitted by law, Customer will reimburse Pinecone for any time expended in assisting Customer with Data Subject Requests under Section 6.1 and in connection with any Customer-initiated audit under Section 7.4, in each case at Pinecone's then current professional service rates, which will be made available to Customer upon request.

14.3 Notices. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Pinecone to Customer under this DPA may be given (a) in accordance with any notice clause of the Agreement, (b) to Pinecone's primary points of contact with Customer, (c) to any email provided by Customer for the purpose of providing it with Services-related communications or alerts, or (d) as provided in Section 5 with respect to the notices contemplated therein. Customer is solely responsible for ensuring that its email addresses are valid.

14.4 Conflict. In the event of any conflict between this DPA and any data privacy provisions set out in any agreements between the Parties relating to Services, the Parties agree that the terms of this DPA shall prevail, provided that if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses control and take precedence. If the Parties have entered into a Business Association Addendum or Agreement with respect to the processing Personal Information regulated by the U.S. Health Insurance Portability and Accountability Act (a "*BAA*"), and there is any conflict between this DPA and the BAA, then the BAA shall prevail, but solely with respect to such regulated Personal Information.

14.5 Severability; Interpretation. If any provision of this DPA is held invalid or unenforceable, the remainder of the Agreement shall continue in full force and effect. The headings in this DPA are for reference only and shall not affect the interpretation of this DPA. For purposes of this DPA, the words "include," "includes" and "including" are deemed to be followed by the words "without limitation"; the word "or" is not exclusive; and the words "herein," "hereof," "hereby," "hereto" and "hereunder" refer to this DPA as a whole.

14.6 Governing Law. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

14.7 Survival. The obligations placed upon each Party under this DPA and the Standard Contractual Clauses shall survive so long as Pinecone processes Customer Personal Data on behalf of Customer.

15. **Changes to DPA**. Pinecone may modify this DPA at any time by posting a revised version at https://www.pinecone.io/legal/data-processing-addendum/ or a successor website designated by Pinecone, provided that the modifications (a) do not materially diminish the overall security of Services used by Customer during the

applicable Subscription Term, (b) do not change the scope of Pinecone's processing of Customer Personal Data, and (c) do not have a material adverse effect on Customer's rights under this DPA. Pinecone may additionally modify this DPA at any time as required to comply with Applicable Law

---

SCHEDULE 1

DETAILS OF PROCESSING AND TRANSFERS

Annex I.A. – List of Parties

Data Exporter

Name	Customer
Address	Address associated with Customer's Pinecone account, or as otherwise specified in this DPA or the Agreement
Contact	Contact details associated with Customer's Pinecone account, or as otherwise specified in this DPA or the Agreement
Activities relevant to data transferred	See Annex I.B. below
Signature and date	See signature page of this DPA
Role	Controller (for Module 2) or processor (for Module 3)

Data Importer

Name	Pinecone Systems, Inc.
Address	1375 Broadway, 11th Fl, New York, NY 10018
Contact	privacy@pinecone.io

Activities relevant to data transferred	See Annex I.B. below
Signature and date	See signature page of this DPA
Role	Processor

Annex I.B. – Description of Transfer

Subject matter	Customer Personal Data
Categories of data subjects whose personal data is transferred	The categories of data subjects whose personal data are transferred are determined solely by Customer. In the normal course of Customer's use of Services, the categories may include employees, agents, advisors, freelancers of Customer (who are natural persons) and End Users.
Categories of personal data transferred	The categories of personal data transferred are determined solely by Customer. In the normal course of Customer's use of Services, the categories of personal data transferred may include name, email address, telephone and title.
Sensitive data transferred	Pinecone does not knowingly collect, and Customer is contractually prohibited from including, any sensitive data or any special categories of data (as defined in European Data Protection Laws) in Customer Personal Data.
Frequency of the transfer	Continuous with use of Services.
Nature of processing	Provision of Services to Customer in accordance with the Agreement, including this DPA. Customer acknowledges that Customer Personal Data is generally processed on an automated, unmonitored basis in accordance with Customer's use of Services.
Purposes of the data transfer and further processing	Provision of Services to Customer in accordance with the Agreement, including this DPA.

Period for which personal data will be retained	During the term of the Agreement and, if applicable, (i) any post-termination retrieval period provided in the Agreement and/or (ii) any further period required by law.

Annex I.C. – Competent Supervisory Authority

Customer agrees the competent supervisory authority will be the Data Protection Commission (DPC) of Ireland.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Pinecone has implemented technical and organizational measures to ensure an appropriate level of security of its Services and Customer Data, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. Further details are available through the Trust Center.

Where required and applicable, the measures outlined at https://www.pinecone.io/legal/security-measures.pdf will serve as Annex II to the Standard Contractual Clauses.

For the prior version of Pinecone's standard customer personal data processing terms, you may request a copy by emailing legal+onlineterms@pinecone.io.

© Pinecone Systems, Inc. | San Francisco, CA
Pinecone is a registered trademark of Pinecone Systems, Inc.