Pinecone

Last updated: May 24, 2024

Pinecone's 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 on Pinecone's security posture can be found in Pinecone's Trust and Security Center, made available at https://security.pinecone.io/ ("Trust Center").

These Security Measures are subject to technical progress and development and Pinecone may modify these Security Measures from time to time without notice, provided that such updates (1) are equivalent to (or enhance) the overall security of Services used by Customer during the applicable Subscription Term and (2) do not materially diminish the level of protection afforded to Customer Data processed through Services during the applicable Subscription Term.

Capitalized terms used, but not defined, in this document have the meanings assigned to them in the Master Subscription Agreement made available at https://www.pinecone.io/legal/.

Category	Pinecone-Assigned ID	Description
Measures of pseudonymization and encryption of personal data	PCS-1	Pinecone encrypts Customer Data in transit and at rest using industry-standard encryption algorithms that are appropriate for the mechanism of transfer (e.g., TLS 1.3, AES-256).
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	PCS-2	Pinecone has implemented and maintains a risk-based information security program that includes safeguards designed to protect the confidentiality, integrity, and availability of Customer Data. Pinecone performs regular assessments to monitor its information security program to identify risks and ensure controls are operating effectively by performing penetration tests, internal audits and risk assessments.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	PCS-3	Pinecone has implemented and maintains a documented set of disaster recovery policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a disaster.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	PCS-4	Pinecone engages qualified external auditors to perform assessments of its information security program against the SOC 2 AICPA Trust Services Criteria for Security, Availability, and Confidentiality. Assessments will be conducted annually and will result in a SOC 2 Type II report that will be made available through the Trust Center. See also PCS-2.
Measures for user identification and authorization	PCS-5	Access to Customer Data is restricted to authorized Pinecone personnel who are required to access Customer Data to perform functions as part of the provision of Services. Access to Customer Data must be through unique usernames and passwords and multi-factor authentication must be enabled. Access is disabled upon an employee's termination.
Measures for the protection of data during transmission	PCS-6	See PCS-1.

Category	Pinecone-Assigned ID	Description
Measures for the protection of data during storage	PCS-7	See PCS-1 and PCS-3.
Measures for ensuring physical security of locations at which personal data are processed	PCS-8	Services and Customer Data are hosted in AWS, GCP and Azure facilities and protected by those Cloud Providers in accordance with their security protocols. Pinecone will review third-party security certifications of the Cloud Providers on at least an annual basis to ensure that appropriate physical security controls are in place.
Measures for ensuring events logging	PCS-9	All access to information security management systems for Services are restricted, monitored, and logged. At a minimum, log entries include date, timestamp, action performed, and the user ID or device ID of the action performed. All logs are protected from change.
Measures for ensuring system configuration, including default configuration	PCS-10	To prevent and minimize the potential for threats to Pinecone's systems, baseline configurations are required prior to deployment of any infrastructure resource. Systems are centrally managed and configured to detect and alert on suspicious activity.
Measures for internal IT and IT security governance and management	PCS-11	IT security governance and management structures and processes are designed to ensure compliance with data protection principles. Pinecone will have dedicated security professionals responsible for implementing, maintaining, monitoring, and enforcing security safeguards aligned with the information security management system.
Measures for certification/assurance of processes and products	PCS-12	Pinecone's information security framework is based on the AICPA COSO Framework and covers the following areas: security risk management, policies and procedures, security incident management, access controls, vulnerability management, physical security, operational security, corporate security, infrastructure security, product security, business continuity disaster recovery, personnel security, security compliance, and vendor security. See also PCS-4.
Measures for ensuring data minimization	PCS-13	Data collection is limited to the purposes of processing (or the data that Customer chooses to process). Employees are directed to access only the minimum amount of information necessary to perform required functions.
Measures for ensuring data quality	PCS-14	See PCS-2.
Measures for ensuring limited data retention	PCS-15	See PCS-13.
Measures for ensuring accountability	PCS-16	See PCS-4 and PCS-12. In addition, Pinecone has implemented data protection policies and appointed European Data Protection Office and its UK affiliate (https://edpo.com/) as its EU and UK data protection representatives.
Measures for allowing data portability and ensuring erasure	PCS-17	Customer has the ability to manage and initiate the deletion of Customer Personal Data through Services. Pinecone provides a mechanism for individuals to exercise their privacy rights in accordance with applicable law, but will generally refer individuals to the applicable customer as provided in the DPA.

Category	Pinecone-Assigned ID	Description
For transfers to subprocessors, also describe the specific technical and organizational measures to be taken by the subprocessor to be able to provide assistance to the controller and, for transfers from a processor to a subprocessor, to the data exporter	PCS-18	Prior to engaging a proposed new subprocessor, Pinecone conducts a risk assessment of the organization's data security practices. Pinecone will restrict an onward subprocessor's access to Customer Personal Data to that strictly necessary to support the provision of Services, and Pinecone will prohibit the subprocessor from processing the Customer Personal Data for any other purpose. Pinecone will impose contractual data protection obligations, including appropriate technical and organizational security measures, on any subprocessor it appoints that require such subprocessor to protect Customer Personal Data in accordance with Data Protection Laws.