Cultivate Security and Privacy

Last Updated 02-28-2020

Cultivate takes the security and privacy of your data very seriously, with robust policies, controls, and systems in place to keep your information safe and secure.

Cultivate has multiple integration options for organizations, including on-premise, virtual private cloud, and Cultivate's cloud platform (using Amazon Web Services). The below security and privacy whitepaper describes an integration with Cultivate's cloud platform.

People Security

All Cultivate employees are required to understand and follow strict internal policies and standards. All employees are trained on security topics including but not limited to device security, preventing spyware/malware, physical security, data privacy, account management, and incident reporting.

Application Security

The Cultivate development team follows security best practices. All code is version controlled and goes through peer review and continuous integration tests to screen for potential security issues. Changes to the production environment are logged and the development team is notified of each release.

Authentication

Cultivate users login with their Google or Office 365 accounts using OAuth 2.0, an industry standard for authorizing secure access to external apps. Cultivate does not receive or store user passwords at any time. Users may revoke Cultivate's access at any time and also are able to request their data be deleted.

Network Security

Encryption in transit

All data in transit between users, Cultivate, and email/messaging services is encrypted using 256-bit SSL/TLS. These protocols are revised as new threats and vulnerabilities are identified.

Network Isolation

Cultivate divides its systems into separate networks using logically isolated Virtual Private Clouds in Amazon Web Services data centers. Systems supporting testing and development activities are hosted in a separate network from systems supporting Cultivate's production services. Customer data only exists and is only permitted to exist in Cultivate's production network. Network access to Cultivate's production environment is restricted. Only network protocols essential for delivery of Cultivate's service to its users are open at Cultivate's perimeter. All network access between production hosts is restricted using firewalls to only allow authorized services to interact in the production network.

Physical Security

Data center security

Cultivate's infrastructure is built on top of Amazon Web Services, and is housed in data centers operated by Amazon. Amazon has strict policies for physical security, including 24-hour video surveillance and strict access restrictions which are described in detail here: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Office security

All employee devices must meet our security standards. These standards require all computers to have strong passwords, encrypt data on disk, run anti-virus software, and lock automatically when idle. No data is stored on employee computers or servers in the office.

Data Security

Data We Collect

Upon authorization by each individual user, Cultivate collects both metadata and content of messages and events in their connected email, messaging, and calendar accounts. The content of events and messages is retained for one year from their dates, but metadata including the registration details, people involved, and length of the message may be retained for the entire time the user has authorized Cultivate. Additionally, we may store the output of classification algorithms run on individual messages indefinitely, however these algorithms contain no personally identifiable information. Lastly, any cookies or other online identifiers including unique IDs, IP addresses, device information and PII derived therefrom shall be retained for up to 90 days.

When Cultivate removes data according the above retention policy, PII will be removed from the running database by deleting the affected rows. All database backups are securely deleted after 7 days.

Cultivate strives for lean analysis of data, and only collects data that is necessary for processing purposes. Cultivate reviews our data collection processes on a quarterly basis to ensure we only collect data that is necessary to provide the services to the user. In addition, Cultivate's Data Protection Officer reviews all products and services with respect to data collection during the design phase. All data must be processed in accordance with authorized purposes which are documented in Cultivate's records of processing. Cultivate's records of processing are only updated by Cultivate's Data Protection Officer.

An individual can request confirmation of whether or not personal information has been collected or held about the requesting individual by sending an email to info@CultivateAI.com. Cultivate will respond to all such requests and provide confirmation within 30 days.

Data Sharing

We do not share or transfer personal identifiable information or the content of any user's messages with any party, including the user's employers, except as required by law or as needed for the purposes of collection or related to providing the Service to users. A user's employer will have access to reports based on metadata, computed statistics, and classifications aggregated over many messages, but the content of any individual message will not be exposed.

Cultivate contracts with Processors shall contain clauses which guarantee data subjects the access rights afforded by the EU-U.S. and Swiss-U.S. Privacy Shield Principles. This includes but is not limited to (i) requiring that processors notify Cultivate of request received directly from the data subject and (ii) deal promptly and properly with all inquiries from Cultivate relating to processor's processing of the personal data subject to the transfer.

Cultivate continuously reviews data transfer procedures to Processors and Controllers to ensure the transfer of personal identifiable information is limited to fulfilling purposes of collection or related purposes only.

Data Access

To the extent possible, Cultivate automates access to customer data and strictly limits viewing by humans. Only Cultivate's Chief Technology Officer and Chief Data Scientist may request permission to access customer data for essential job functions for a limited amount of time in a secure environment. All requests to access customer data must be reviewed and approved by the executive team and must have a clear technical justification. Cultivate reviews access and security audit logs on a regular basis.

At any time, a user may request access to the personal identifiable information collected about them by sending an email to info@CultivateAI.com with the subject line "Data Access Request". Cultivate will verify the email matches the email that was authorized with the Cultivate platform before providing access. Cultivate will respond to all Data Access Requests within 30 days. If access is refused, Cultivate will provide the requesting-individual with an explanation of why access will not be provided, together with contact information for further inquiries about the denial of access. Upon request, Cultivate will provide confirmation of whether or not PI is being processed about the requesting individual.

Data Removal

At any time, a user may stop using the Service and request for a full removal of their data (via an e-mail to info@CultivateAI.com or clicking on the "delete account" link in their user settings tab from their Cultivate account). Clicking the "delete account" link will trigger an email to Cultivate's CTO to start the account delete process. Within a period of 30 days, all of the user's messaging content and PII will be removed from the running database by deleting the affected rows. All database backups are securely deleted after 7 days.

Data Correction

If a user believes their data stored on Cultivate is incorrect, they, at any time, may contact us and request their data to be corrected by sending an email to info@CultivateAI.com with the subject line "Information Correction Request". Cultivate will respond to all Data Correction Requests within 30 days. If correction is refused, Cultivate will provide the requesting-individual with an explanation of why correction will not be provided, together with contact information for further inquiries about the denial of correction.

Cultivate will reply to all Information Correction Request emails within 30 days and provide a confirmation that the information has been corrected or deleted.

Encryption at rest

All data at rest in Cultivate's production network is encrypted using 256-bit Advanced Encryption Standard (AES). Message content is further encrypted in our database such that the plaintext never exists on Cultivate database servers at any point in time. Cultivate uses the AWS Key Management Service (KMS) to manage encryption keys. Keys are never stored on disk and retained only in memory while in use. Encryption keys are rotated regularly.

Server hardening

Production servers are hardened, with the minimally required set of services allowed to run. A custom based server image which has been reviewed for security is used to run all production services.

Vulnerability Management

Cultivate uses third party services to run automated vulnerability tests on the production environment. Engineers are always on call to immediately address any issues.

Penetration testing

Cultivate undergoes independent black and gray box security penetration tests by third-party security firms. The findings are reviewed, prioritized, and tracked to resolution, including third-party verification of resolution.

Compliance

Cultivate requires all contracts with Data Processors to include the below provisions as required by the Privacy Shield Framework:

- You are transferring the data to the Processor only for limited and specified purposes
- The Processor is obligated to provide at least the same level of privacy protection as is required by the Privacy Shield Principles
- The Processor is required to take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with your organization's Privacy Shield obligations
- The Processor is required to notify your organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles
- Upon notice, the Processor is required to take reasonable and appropriate steps to stop and remediate unauthorized processing

Cultivate is hosted in Amazon Web Services (AWS) data centers, which are certified to meet compliance requirements of SOC2 and ISO27001. Details can be found at https://aws.amazon.com/compliance/.

To request a copy of Cultivate's SOC2 report or Security Policies (including Change Management, Incident Management, etc.) please send a request to info@CultivateAI.com.

At any time, a user may submit a Privacy Shield related complaint or question by sending an email to info@CultivateAI.com. All Privacy Shield related complaints or questions will be responded to within a period of 30 days.