Pypestream Data Security & Privacy Policy

Last Updated: April 30, 2019

Pypestream Inc., its subsidiaries and affiliates (collectively “we” “us” or “Pypestream”) respect your privacy. This Privacy and Data Security Policy (“DSP”) applies to how we collect, use, disclose, and secure Personal Information (defined below) obtained:

1. On pypestream.com, downloadable iOS and Android Pypestream applications, and any other web applications (our “Site”) from users (“Site Users”);

2. Through organizations that use our technology (“Platform Customers”) to communicate with their employees, customers, end-users or audience (“Platform End Users”, and together with Site Users and Platform Customers, “All Users”) through our messaging platform (“Cloud Service”); and

3. Through any additional products or services offered by Pypestream (together with the Site and Cloud Service, the “Service”).

Agreements between individual Platform Customers and Pypestream, including applicable Cloud Service Agreements (“CSA”) or Order Forms may specify additional rights or obligations with respect to Personal Information.

“Personal Information” means information that alone or when in combination with other information may be used to readily identify, contact, or locate an individual, such as: name, social security number, address, email address, location, or phone number.

The Cloud Service provides an online platform for the creation and sharing of materials, ideas, concepts and communications between Platform Customers and Platform End Users via online conversations, called "Sessions," which are contained within secure, bidirectional connections associated with a given Platform Customer or subject matter, called "Pypes". Personal Information may be obtained in the creation and sharing of Sessions and Pypes as described below. We follow generally accepted standards to protect the Personal Information submitted to us, both during transmission and once it is received through a Session.

This DSP describes the choices All Users have regarding our collection and use of Personal Information. However, we are not responsible or liable for (and this DSP does not apply to) the privacy practices or content of any third-party sites linked through Pypestream, including but not limited to those of Platform Customers, since we do not control them. Platform Customers may be able to: (i) restrict, suspend or terminate your access to the Service; (ii) access and describe Personal Information that you provided to them through the Service; (iii) access and export Personal Information processed by them; and (iv) amend or retain your Personal Information (including after we no longer retain it). Platform Customers are solely responsible for ensuring compliance with all applicable laws and regulations, as well as any privacy policies, agreements or other obligations, relating to the collection of Personal Information in connection with the use of the Cloud Service by Platform End Users. This includes but is not limited to data protection laws relating to Platform Customers' role as the data controller for Platform End Users. We collect information under the direction of our Platform Customers, and may have no direct relationship with individuals whose Personal Information we process in connection with our Platform Customers' use of the Cloud Service. The use of information collected through the Cloud Service is limited to the purpose of providing the service for which Platform Customers have engaged Pypestream in an applicable CSA or Order Form. If you are an individual who interacts with a Platform Customer, and would either like to amend your contact information or no longer wish to be contacted by that Platform Customer, or have other requests or questions relating to your Personal Information, please contact the Platform Customer that you interact with directly.

This DSP is incorporated by reference into our Terms of Use (and together with this DSP, the "Terms"). Any capitalized terms used and not defined in this DSP shall have the meaning given to them in the Terms of Use.

Privacy

1. WHAT INFORMATION DO WE COLLECT?

We collect various kinds of information, some of which is Personal Information, and some of which is non-identifying or aggregated. We may receive Personal Information or other information in a variety of ways described below, based on access granted to us by Site Users and Platform Customers.

a. Registration and Account Information

If you engage or register with the Cloud Service through a Platform Customer, we may collect information needed to register or create an account. In order to create a Pypestream account we may ask for and may collect a username, a password, an email address, a phone number, and other information. Further information you may choose to provide to us is optional and provided at your discretion.

We may also collect information regarding the relationship between Platform Customers and individual Platform End Users within a given Pype or Session. We also collect all information provided by Platform Customers in relation to the distribution of invitations to Platform End Users to join Pypestream and information provided to us by Platform Customers for the purposes of onboarding Platform End Users.

b. Platform Customer billing information

We collect billing and payment information from Platform Customers, which is securely passed to our payment processing partners, but is stored exclusively and securely within Pypestream's accounts payable systems.

c. Log data and Cookies

When All Users use the Service, our servers automatically record information, including information that internet browsers send whenever you visit a website or that your mobile app sends when using it. This log data may include your IP address, your browser type and settings, the date and time of your request, information about your browser configuration and plug-ins, language preferences and cookie data. When you visit our Site, use our Cloud Services or open our emails, we, our Platform Customers, and our third-party partners, such as social media widgets, and analytics providers, may collect certain information by automated means, such as cookies, web beacons and web server logs.

Cookies are small text files we send to your computer and that your computer sends to us, each time you use the Service. They are unique to your Pypestream account or your browser. Pypestream uses cookies to record log data. We use both session-based and persistent cookies. Session-based cookies last only while your browser is open, and are automatically deleted when you close your browser. Persistent cookies last until you or your browser delete them or until they expire. Some cookies are associated with your Personal Information in order to remember that you are logged in. Other cookies are not tied to your Pypestream account but are unique and allow us to perform of collect site analytics and customize the user experience, among other things. If you access the Service through your browser, you can manage your cookie settings there, but if you disable all cookies you may not be able to use some or all of the Service. Pypestream sets and accesses our own cookies on our company-owned domains. In addition, we use third parties, like Google Analytics, for analytics on the Service. To learn more about Google Analytics and how to opt-out, please visit www.google.com/policies/privacy/partners/. Our Service responds to browser Do-Not-Track signals, however our Site does not.

d. Device/Usage information

In addition to log data, we may also collect information about the device you're using the Service on, including what type of device it is, what operating system you're using, device settings, unique device identifiers, and crash data.

e. Geolocation information

Precise GPS locations from mobile devices may be collected only with your permission if device settings are enabled to send it to us. WiFi and IP addresses received from your browser or device may also be used to infer approximate location (only with consent).

f. Pypestream usage information

This is information about which Platform Customers, features, content, and links a Platform End User interacts within a given use of the Service. We use this information for internal and service-related purposes.

g. Pypestream communications and content

We may collect communications that All Users send and receive within the Service, including but not limited to in any Pypes or Sessions. This includes messages, pictures, files and video, the time messages or files were sent and by whom, when or if they were seen by you, and where you received them, or other information related to your browsing, purchasing and online behavior and activities with respect to a particular Platform Customer.

h. Information from partners or other third parties

Pypestream may receive information from partners or others that we could use to improve and enhance our products. This might be aggregate level information about which IP addresses match to which zip codes or it might be more specific information about how well an online marketing or email campaign performed.

2. HOW DO WE USE YOUR INFORMATION?

a. To provide and secure the Service

We use information you provide (including Personal Information, to the extent applicable) to authenticate you, and to deliver message content to you and from you. For instance, we use registration and account information to facilitate Sessions between Platform Customers and Platform End Users, and to ensure that Platform End Users are connected to the correct Pype based on the Platform Customer that they want to contact. We also use log data, such as IP address, to authenticate Platform End Users entering individual Sessions within Pypes with our Platform Customers, and to end Sessions that are idle or inactive. We also continuously take the steps necessary to keep Pypestream secure, to prevent abuse and fraud and to ensure the integrity of the Service as detailed in the “Data Security” section below.

b. To understand and improve the Service

We utilize usage information in various ways to improve, iterate and enhance our product. For instance, we may use aggregated or anonymized usage data regarding the efficiency and effectiveness of a given Session to help our Platform Customers improve their levels of customer service through their Pypes. When we anonymize or aggregate data collected through the Service, we may use and disclose it for any purpose.

c. To communicate with you

We will use your information to respond to support queries and address your problems or concerns. We may communicate with you within the Service, or we may send you service or administrative emails when necessary. We may also contact you to inform you about changes to our terms or service offerings.

3. DISCONNECTING FROM PYPES AND SESSIONS; DELETING PLATFORM END USER ACCOUNTS

Sessions between Platform End Users and Platform Customers are time-limited and are disconnected once left idle or inactive. Platform Customers may deactivate their Platform End User accounts by sending a deactivation request to our Customer Experience and Success Team. Deactivation of an account disables Platform End User access to the Pypestream content associated with that account, but does not delete such content and does not affect the relationship or obligations between a Platform Customer and Pypestream established through an applicable CSA or Order Form.

4. HOW DO WE SHARE AND/OR DISCLOSE INFORMATION WE COLLECT?

a. To comply with legal/law enforcement requests and protect our rights.

Pypestream may access, preserve, and disclose your information in cases where we believe doing so is reasonably necessary to: (i) comply with a law, regulation or legal request; (ii) to protect the safety, rights, or property of the public, any person, or Pypestream; or (iii) to detect, prevent, or otherwise address fraud, security or technical issues.

b. With our Vendors and Service Providers.

Our third-party service providers who provide hosting and maintenance for the Service, development, backup, storage, payment processing, analytics and other services may have access to Personal Information. Their access may include processing of your Personal Information, as a sub-processor of Pypestream, for the purpose of providing services based on our instructions, and in compliance with this DSP. We do not permit our third-party service providers to use the Personal Information that we share with them for their marketing purposes or for any other purpose than in connection with the services they provide to us and under contractual promises of confidentiality.

c. As part of a merger, sale, or other asset transfer.

If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, sale of company assets, or transition of service to another provider, your information may be disclosed in connection with the negotiation of such transaction, and/or sold or transferred as part of such a transaction as permitted by law and/or contract.

d. As aggregated or anonymized data.

We may share aggregated anonymized information with our partners or others for business or research purposes. For example, we may share usage statistics and advanced analytics with customers or potential customers or research partners. We may also share data regarding the effectiveness and efficiency of a given Session or Pype with the Platform Customer that owns that Session or Pype in order to improve their customer service capabilities.

e.With Your Permission.

We may also disclose your information with your permission.

5. DATA RETENTION AND INTERNATIONAL DATA TRANSFER

If you are using the Service, you agree to the transfer of your Personal Information to the United States and processing globally by providing us with that information. If you are a visitor from the European Economic Area, our legal basis for collecting and using the Personal Information described above will depend on the Personal Information concerned and the specific context in which we collect it.

You may have certain rights to the Personal Information we hold about you, including the right to access such Personal Information, the right to receive a copy of Personal Information provided to and processed by us, and to correct Personal Information that is inaccurate. Platform End Users can also delete their accounts or remove certain Personal Information. Some of these only apply in certain circumstances (as set out in more detail below) and as provided under EU data protection laws.

Generally, we retain Personal Information only as long as required to perform our Services or other purpose that was the reason for the collection of the information. We will normally collect Personal Information from you only where we need the Personal Information to provide our Service, where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms, or where we have your consent. In some cases, we may also have a legal obligation to collect Personal Information from you. If we ask you to provide Personal Information to comply with a legal requirement or to perform a contact with you, we will make this clear at the relevant time. If we process Personal Information in reliance on your consent, you may withdraw your consent at any time.

We do not share your Personal Information with third parties, unless it is necessary to carry out your request, for our professional or legitimate business needs, or as required or permitted by law. When we transfer your Personal Information to third parties or service providers, contractual arrangements will be established for data processing in compliance with applicable data protection law.

Where Pypestream is the data controller of Personal Information (for example, Personal Information relating to Site Users or Platform End Users who register for an account directly with us), we retain the Personal Information we collect where we have an ongoing legitimate business need to do so (for example, to provide you with the Service and to comply with applicable legal, tax or accounting requirements). When we have no ongoing legitimate business need to process your Personal Information, we will either delete or aggregate it. We remove information from our computing resources upon the expiration or cancellation of the Service, or earlier upon request from a Platform

Customer or Site User, as applicable. Pypestream does not archive information from Users, however some information may remain in backup files until expiration of such files as governed by Pypestream's backup retention practices. When destroying Personal Information, measures will be taken to make the Personal Information irrecoverable or irreproducible, and electronic files which contain Personal Information will be deleted permanently. If immediate deletion is not possible (for example, because your Personal Information has been stored in backups), then we will securely store your Personal Information and isolate it from any further processing until deletion is possible. If you have the right to request and require Pypestream to destroy your Personal Information before the end of its life cycle, Pypestream will destroy your Personal Information in accordance with applicable data protection law. All Site Users or Platform End Users who request Pypestream to destroy their Personal Information should also promptly make the same request to the applicable Platform Customer they interacted with as such Platform Customer may be retaining copies of such Personal Information, as detailed on the first page of this DSP, and any such retention is outside the control of Pypestream.

We may need to retain Personal Information if there are valid grounds under data protection laws for us to do so (e.g., for the defense of legal claims or freedom of expression) but if you have the right to request and ask us to destroy Personal Information, we will let you know if that is the case. Where you have the right and have requested that we erase Personal Information that has been made available publicly, and there are grounds for erasure, we will use reasonable steps to try to tell others that are displaying the Personal Information or providing links to the Personal Information to erase it too.

You may have a right to require us to stop processing the Personal Information we hold about you other than for storage purposes in certain circumstances. Please note, however, that if we stop processing the Personal Information, we may use it again if there are valid grounds under data protection laws for us to do so (e.g., for the defense of legal claims or for another's protection). As above, where we agree to stop processing the Personal Information, we will try to tell any third party to whom we have disclosed the relevant Personal Information so that they can stop processing it too.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us via the channels below.

6. CALIFORNIA PRIVACY RIGHTS

California Civil Code § 1798.83 permits our users who are California residents to request certain information regarding our disclosure of Personal Information to third parties for their direct marketing purposes. We do not share our users' Personal Information with unaffiliated third parties for their direct marketing purposes without our users' consent. However, if you are a California resident and you have any questions about our disclosure of your Personal Information to third parties, please contact us via the channels below.

7. CHILDREN'S INFORMATION

We do not knowingly collect, maintain, or use Personal Information from children under 13 years of age, and no part of Pypestream is directed to children under the age of 13. If you learn that your child has provided us with Personal Information without your consent, you may alert us via the channels below. If we learn that we have collected any Personal Information from children under 13, we will promptly take steps to delete such information and terminate the child's account.

Data Security

1. SECURITY FEATURES

Pypestream takes reasonable steps to protect information provided to us from loss, misuse, and unauthorized access or disclosure. When we are provided with sensitive information (such as sign-in credentials), we encrypt the transmission of that information using secure socket layer technology (SSL). Pypestream encrypts data in transit to and from data centers in and at rest. Pypestream also encrypts all data at rest. We follow generally accepted standards to protect the personal data submitted to us, both during transmission and once we receive it. However, no electronic transmission or digital storage mechanism is ever totally secure or error-free.

2.PLATFORM CUSTOMER AND PLATFORM END USER CONTENT SECURITY

Additional security measures for the Cloud Service are governed by an applicable CSA or Order From between Pypestream and individual Platform Customers. Pypestream's security is designed to protect information that Platform Customers input into the Cloud Service (including from Platform End Users) ("Content") and to maintain the availability of such Content.

3. DATA PROCESSING

To the extent applicable, Platform Customers are the sole controller for any personal data included in the Content, and appoint Pypestream as a processor to process such personal data (as those terms are defined in the General Data Protection Regulation ((EU) 2016/679) (GDPR)). Per California law, Pypestream adheres to the California Consumer Privacy Act as of January 1, 2020.

4. CONFIDENTIALITY

Pypestream does not disclose Content except to Pypestream employees, contractors, and subprocessors, and only to the extent necessary to deliver the Cloud Service, unless otherwise specified in an applicable CSA between an individual Platform Customer and Pypestream.

Our third-party data center provider (AWS) (as described in our "Physical Security and Entry Control" section below) will sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization and their own internal policies for physical media.

a. Upon request from a Platform Customer, Pypestream will provide evidence of stated compliance and accreditation, such as certificates, attestations, or reports resulting from accredited independent third-party audits. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain the Cloud Service's stated compliance and accreditation.

b. Data collected through Cloud Services is considered confidential between Pypestream and individual Platform Customers, and is not sold to any third party companies.

c. Pypestream encrypts all data obtained as described in this DSP. Upon request from individual Platform Customers from whom data has been obtained through Cloud Services, Pypestream will destroy requested user data within 30 days of initial request.

d. To facilitate our global operations, we transfer information to either European Union or the United States and allow access to that information from countries in which Pypestream operates in for the purposes described in this DSP. These countries may not have equivalent privacy and data protection laws to the laws of many of the countries where our Platform Customers or Site Users are based. When we share information within Pypestream, we make use of standard contractual data protection clauses, which have been approved by the European Commission, and we rely on the EU-U.S. and Swiss-U.S. Privacy Shield Framework to safeguard the transfer of information we collect from the European Economic Area and Switzerland.

Privacy Shield

a. Pypestream Inc. participates in and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the Privacy Shield Principles regarding the collection, use, and retention of information about you that is transferred from the European Union or Switzerland (as applicable) to the U.S. We ensure that the Privacy Shield Principles apply to all information about you that is subject to this privacy DSP and is received from the European Union, the European Economic Area, and Switzerland.

b. Under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, we are responsible for the processing of information about you we receive from the EU and Switzerland, and onward transfers to a third party acting as an agent on our behalf. We comply with the Privacy Shield Principles for such onward transfers. We remain liable in accordance with the Privacy Shield Principles if third-party agents that we engage to process such information about you on our behalf do so in a manner inconsistent with the Privacy Shield Principles, unless we prove that we are not responsible for the event giving rise to the damage.

Security Policies

a. Pypestream will maintain and follow IT security policies and practices that are integral to Pypestream's business and mandatory for all Pypestream employees and contractors.

b. Pypestream will review its IT security policies at least annually and amend such policies as Pypestream deems reasonable to maintain protection of the Cloud Services.

c. Pypestream will maintain and follow its standard mandatory employment verification requirements for all new hires, including contract employees, and extend such requirements to wholly owned Pypestream In accordance with Pypestream internal process and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by Pypestream.

d. Pypestream employees will complete security and privacy education annually and certify each year that they will comply with Pypestream's ethical business conduct, confidentiality, and security policies, as set out in Pypestream's Code of Conduct and various security policies.

Security Incidents

a. Pypestream will maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling, and will comply with data breach notification terms of an applicable CSA or under applicable data breach notification laws.

b. Pypestream will investigate unauthorized access and unauthorized use of Content of which Pypestream becomes aware (security incident), and, within the Cloud Service scope, Pypestream will define and execute an appropriate response plan. Platform Customers must also notify Pypestream of any suspected vulnerability or incident of which they become aware.

Access, Intervention, Transfer and Separation Control

a. Pypestream will maintain documented security architecture of networks managed by Pypestream in its operation of the Cloud Service. Pypestream will separately review such network architecture standards in-depth prior to implementation, including measures reasonably designed: (i) to prevent unauthorized network connections to systems, applications and network devices; and (ii) for compliance with its secure segmentation, isolation, and defense. Pypestream may use wireless networking technology in its maintenance and support of the Cloud Service and associated components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to Cloud Service networks. Cloud Service networks do not use wireless networking technology.

b. Pypestream will maintain measures for the Cloud Services that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons.

c. To the extent described in the relevant CSA, Pypestream will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, and FTPS, for individual Platform Customer’s secure transfer of Content to and from the Cloud Service over public networks. If the Cloud Service includes management of cryptographic keys, Pypestream will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

d. If Pypestream requires access to Content, Pypestream will restrict and limit such access to the lowest level required to provide and support the Cloud Service. Such access, including administrative access to any underlying components (privileged access), will be individual, role based, and subject to approval and regular validation by authorized Pypestream personnel following the principles of segregation of duties. Pypestream will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or request of authorized Pypestream personnel, such as the account owner's manager.

e. Consistent with industry standard practices, and to the extent natively supported by each component managed by Pypestream within the Cloud Service, Pypestream will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

f. Pypestream will monitor use of privileged access and maintain security information and event management measures designed to a) identify unauthorized access and activity, b) facilitate a timely and appropriate response, and c) to enable internal and independent third party audits of compliance with documented Pypestream DSP.

g. Logs in which privileged access and activity are recorded will be retained in compliance with Pypestream's audit policies. Pypestream will maintain measures designed to protect against unauthorized access, modification and accidental or deliberate destruction of such logs.

h. To the extent supported by native device or operating system functionality, Pypestream will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature based malware detection and removal, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

Service Integrity and Availability Control

a. Pypestream: (i) enlists a qualified independent third-party to perform penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter; (ii) performs automated management and routine verification of underlying components' compliance with security configuration requirements; and (iii) remediates identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. Pypestream will take reasonable steps to avoid Cloud Service disruption when performing its tests, assessments, scans, and execution of remediation activities.

b. Pypestream will maintain policies and procedures designed to manage risks associated with the application of changes to its Cloud Services. Prior to implementation, changes to the Cloud Service, including its systems, networks and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Cloud Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

c. Pypestream will maintain an inventory of all information technology assets used in its operation of the Cloud Service. Pypestream will continuously monitor the health and availability of the Cloud Service and underlying components.

d. Pypestream will maintain measures designed to assess, test, and apply security advisory patches to the Cloud Service and its associated systems, networks, applications, and underlying components within the Cloud Service scope. Upon determining that a security advisory patch is applicable and appropriate, Pypestream will implement the patch pursuant to documented severity and risk assessment guidelines. Implementation of security advisory patches will be subject to Pypestream change management DSP.

Physical Security and Entry Control

Pypestream's Cloud Infrastructure runs on our third-party data center provider, Amazon Web Service (AWS) using AWS Virtual Private Cloud. AWS security standards for physical infrastructure are defined in AWS: Overview of Security Process the latest version of AWS Security Policies are available here: https://aws.amazon.com/security/

Changes to this DSP

From time to time this DSP may be amended or updated. By continuing to use Pypestream after those changes are in effect you agree to the revised DSP.

Contact Us:
Pypestream Inc.
122 West 26th Street, 2nd Floor
New York, NY

866.444.PYPE (7973)