Data Protection Agreement ("DPA")

The parties agree that this Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data and Personal Data in connection with the Services.

In the event of any conflict or inconsistency between this DPA and any other terms set forth in the applicable Master Subscription License Agreement (the "Agreement"), this DPA shall prevail.

For clarity, the Standard Contractual Clauses prevail over any other term of the DPA.

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the Agreement. The following defined terms are used in this DPA:

"Customer Data" means all data, including all files, text, sound, video, or image files that are provided to PoliteMail by, or on behalf of, Customer through use of the Service.

"CCPA" means the California Consumer Protection Act of 2018.

"Diagnostic Data" means data collected or obtained by PoliteMail from software that is locally installed by Customer in connection with the Service. Diagnostic Data does not include Customer Data or Service Generated Data.

"Data Protection Requirements" means the CCPA, GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Local EU/EEA Data Protection Laws" means any subordinate legislation and regulation implementing the GDPR.

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Service Generated Data" means data generated or derived by PoliteMail through the operation of an Service. Service Generated Data does not include Customer Data or Diagnostic Data.

"Standard Contractual Clauses" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. When required the Standard Contractual Clauses are attached hereto as an Exhibit.

"Subprocessor" means other processors used by PoliteMail to process Customer Data and Personal Data, including any subcontractor that processes Customer Data and Personal Data.

"Support Data" means all data, including all files, text, sound, video, image files, or software, that are provided to PoliteMail by or on behalf of Customer (or that Customer authorizes PoliteMail to obtain from an Service) through an engagement with PoliteMail to obtain technical support for Services covered under this agreement.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms "data importer" and "data exporter" have the meanings given in the Standard Contractual Clauses.

General Terms

Compliance with Laws

PoliteMail will comply with all laws and regulations applicable to its provision of the Services, including security breach notification law and Data Protection Requirements. However, PoliteMail is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. PoliteMail does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements.
Customer is responsible for determining whether the Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of an Service, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

Scope; The terms in this DPA apply to the Services.

Nature of Data Processing; Ownership

PoliteMail will use and otherwise process Customer Data and Personal Data only (a) to provide Customer the Services in accordance with Customer's documented instructions, and (b) for PoliteMail's legitimate business operations, each as detailed and limited below. As between the parties, Customer retains all right, title and interest in and to Customer Data. PoliteMail acquires no rights in Customer Data, other

than the rights Customer grants to PoliteMail in this section. This paragraph does not affect PoliteMail's rights in software or services PoliteMail licenses to Customer.

Processing to Provide Customer the Services

For purposes of this DPA, "to provide" a Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, investigating and repairing issues and problems); and
- Ongoing improvement (installing the latest updates, making improvements to user productivity, reliability, efficacy, and security).
- Monitoring systems and user performance, including license utilization, system data processing, and statistical data processing.

When providing Services, PoliteMail will not use or otherwise process Customer Data or Personal Data for advertising or similar commercial purposes unless such use or processing is in accordance with Customer's documented instructions.

Processing for PoliteMail's Legitimate Business Operations

For purposes of this DPA, "PoliteMail's legitimate business operations" consist of the following, each as incident to delivery of the Services to Customer: (1) licensing, billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect PoliteMail or the Service; (5) improving the core functionality of systems performance, accessibility, privacy or energy-efficiency; (6) statistical benchmarking; (7) training of machine learning models utilized to provide particular features of the Services; and (8) financial reporting and compliance with legal obligations (subject to the limitations on disclosure outlined below).

Disclosure of Customer Data and Third-Party Requests

PoliteMail will not disclose Customer Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. All processing of Customer Data is subject to PoliteMail's obligation of confidentiality under the Master Subscription License Agreement.

If PoliteMail receives any request, inquiry, claim or compliant from a governmental, legislative, judicial, law enforcement or regulatory authority (such as an EU data authority) or other third party with a legitimate demand or claim regarding Customer Data, PoliteMail will attempt to reject such and redirect the third party to the Customer. If compelled to disclose Customer Data by legal order, PoliteMail will promptly notify Customer and provide a copy of such demand unless legally prohibited from doing so.

PoliteMail will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if PoliteMail is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, PoliteMail may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR

All Personal Data processed by PoliteMail in connection with the Services is obtained as either Customer Data, Diagnostic Data, or Service Generated Data. Personal Data provided to PoliteMail by, or on behalf of, Customer through use of the Service is also Customer Data. Pseudonymized identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent PoliteMail is a processor or subprocessor of Personal Data subject to the GDPR, the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and PoliteMail agree that Customer is the controller of Personal Data and PoliteMail is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case PoliteMail is a subprocessor; or (b) as stated otherwise in this DPA.

When PoliteMail acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its Agreement (including this DPA), along with the product documentation and Customer's use and configuration of features in the Services, are Customer's complete and final documented instructions to PoliteMail for the processing of Personal Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to PoliteMail that Customer's instructions, including appointment of PoliteMail as a processor or subprocessor, have been authorized by the relevant controller.

To the extent PoliteMail uses or otherwise processes Personal Data subject to the GDPR or other Data Protection Requirements in connection with PoliteMail's legitimate business operations, PoliteMail will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations. PoliteMail employs safeguards to protect Customer Data and Personal Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the Agreement and DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Service pursuant to the Agreement.
- **Categories of Data.** The types of Personal Data processed by the Service include: (i) Personal Data that Customer elects to include in Customer Data; and (ii) those expressly identified in Article 4 of the GDPR that may be contained in Diagnostic Data or Service Generated Data. The types of Personal Data that Customer elects to include in Customer Data may be any categories of Personal

Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in The Standard Contractual Clauses (Processors).

- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, and collaborators, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix 1 to The Standard Contractual Clauses (Processors).

Data Subject Rights; Assistance with Requests

PoliteMail will make available to Customer, in a manner consistent with the functionality of the Service and PoliteMail's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If PoliteMail receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with Services for which PoliteMail is a data processor or subprocessor, PoliteMail will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Service. PoliteMail shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires PoliteMail to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to PoliteMail and keep it accurate and up-to-date. PoliteMail may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

PoliteMail will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, data transmitted, stored or otherwise processed. Those measures shall be set forth herein as the Technical and Organizational Security Measures (referenced hereto as Appendix AA) and further detailed in the PoliteMail Information Security Policy. PoliteMail will make such policy available to Customer under NDA, along with descriptions of the security controls in place for the Service and other information reasonably requested by Customer regarding PoliteMail security practices and policies.

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for the Service meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by PoliteMail provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for any components that Customer provides or controls.

Auditing Compliance

PoliteMail will conduct routine assessments of the security controls that it uses in conjunction with the processing of Customer Data and Personal Data, as follows:

- Implement a control standard or framework and perform assessments according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

- An independent third party shall annually attest to the implementation of such applicable control standard or framework. An independent third party shall perform a manual application penetration test to evaluation the efficacy of such security control protocols.

PoliteMail shall remediate all medium or higher risk issues raised in any such assessment the satisfaction of the assessor, whether internal or external. All low-risk items shall be addressed in written form, with remediation plans or schedules where applicable.

To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through the reports, documentation or compliance information PoliteMail makes generally available to its customers, PoliteMail will promptly respond to Customer's additional audit instructions. Customer may elect to perform it's own audit, at its own expense. Before the commencement of an audit, Customer and PoliteMail will mutually agree upon the scope, timing, duration, control and evidence requirements, provided that this requirement to agree will not permit PoliteMail to unreasonably delay performance of the audit. To the extent needed to perform the audit, PoliteMail will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by PoliteMail, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to PoliteMail, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from PoliteMail's other customers or data or to PoliteMail systems or facilities not involved in the Services.

Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time PoliteMail expends for any such audit, in addition to the rates for services performed by PoliteMail. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with PoliteMail and PoliteMail shall promptly cure any material non-compliance.

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements.

Security Incident Notification

If PoliteMail becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by PoliteMail (each a "Security Incident"), PoliteMail will promptly and without undue delay and within 24 hours (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to the administrator identified by Customer and by any means PoliteMail selects, including via phone and email. It is Customer's sole responsibility to ensure that PoliteMail has been provided with accurate contact information for Customer's administrator. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

PoliteMail shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

PoliteMail's notification of or response to a Security Incident under this section is not an acknowledgement by PoliteMail of any fault or liability with respect to the Security Incident.

Customer must notify PoliteMail promptly about any possible misuse of its accounts or authentication credentials or any security incident related to a Service.

Data Transfers and Location

Data Transfers

Except as described elsewhere in the DPA, Customer Data and Personal Data that PoliteMail processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which PoliteMail or its Subprocessors operate. Customer appoints PoliteMail to perform any such transfer of Customer Data and Personal Data to any such country and to store and process Customer Data and Personal Data to provide the Services.

The transfer of Personal Data from the European Economic Area ("EEA"), the United Kingdom or Switzerland to a country located outside of the EEA which is not subject to an adequacy decision will be subject to the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as annexed to Commission Implementing Decision 2021/914 ("SCCs"), which are incorporated into this DPA by this reference.

PoliteMail will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

PoliteMail is self-certified to the EU-U.S. Data Privacy Frameworks and the commitments they entail. PoliteMail agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by these Data Privacy principles.

Data Retention and Deletion

At all times during the term of Customer's subscription, Customer will have the ability to access, extract and delete Customer Data stored in each Service.

PoliteMail will retain Customer Data for the term of the Agreement. Customer Data that remains stored in Services shall be retained for 30 days after expiration or termination of Customer's subscription, and during that time Customer may request an extract of the data. After the 30-day retention period ends, PoliteMail will permanently destroy and delete the Customer Data and Personal Data including backups of such data

within an additional 30 days, unless PoliteMail is permitted or required by applicable law, or authorized under this DPA, to retain such data.

PoliteMail has no liability for the deletion of Customer Data or Personal Data as described in this section.

Processor Confidentiality Commitment

PoliteMail will require that its personnel engaged in the processing of Customer Data and Personal Data (i) process such data only on instructions from Customer or as described in this DPA, and (ii) are obligated to maintain the confidentiality and security of such data even after their engagement ends. PoliteMail shall provide periodic and mandatory security awareness training including data privacy awareness to its employees with access to Customer Data and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

PoliteMail may hire third parties to provide certain limited or ancillary services on its behalf. Customer consents to the engagement of these third parties as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by PoliteMail of the processing of Customer Data and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

PoliteMail is responsible for its Subprocessors' compliance with PoliteMail's obligations in this DPA. PoliteMail makes available information about Subprocessors within a Statement of Work. When engaging any Subprocessor, PoliteMail will maintain a written contract that restricts the Subprocessor's access and use of Customer Data or Personal Data only to deliver the services PoliteMail has retained them to provide and prohibits the Subprocessor from using Customer Data or Personal Data for any other purpose. PoliteMail will require Subprocessors to be bound by written agreements that require them to provide at least the level of data protection required of PoliteMail by the DPA. PoliteMail agrees to oversee the Subprocessors to confirm that these contractual obligations are met.

From time to time, PoliteMail may engage new Subprocessors. PoliteMail will give Customer notice (by providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 60 days in advance of providing that Subprocessor with access to Customer Data.

Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, PoliteMail acknowledges that for the purposes of the DPA, PoliteMail is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and PoliteMail agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that PoliteMail may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Service that may be required by applicable law and to convey notification on behalf of PoliteMail to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully- issued subpoena requiring the disclosure of Customer Data in PoliteMail's possession as may be required under applicable law.

California Consumer Privacy Act (CCPA)

If PoliteMail is processing Personal Data within the scope of the CCPA, PoliteMail makes the following additional commitments to Customer. PoliteMail will process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will PoliteMail sell any such data. These CCPA terms do not limit or reduce any data protection commitments PoliteMail makes to Customer in the DPA, or other agreement between PoliteMail and Customer.

How to Contact PoliteMail

If Customer believes that PoliteMail is not adhering to its privacy or security commitments, Customer may contact PoliteMail at:

privacyofficer@politemail.com

securityofficer@politemail.com

Appendix AA – Technical and Organizational Security Measures

PoliteMail shall protect Customer Data, Confidential Information and Personally Identifiable Information through implementation and maintenance of policies and controls in alignment with the most recent versions of the international standard ISO27001. The Technical and Organizational Security Measures, in conjunction with the confidentiality and security commitments of this DPA and any related Master Services Agreement ("MSA", including the GDPR and CCPA Terms if so incorporated), are PoliteMail's only responsibility with respect to the security and privacy of the Customer Data stored and processed by the Services.

http://docs.politemail.com/PoliteMailTechnicalandOrganizationalSecurityMeasures.pdf