Data Processing Addendum
Mailstream on Demand UK (06.24)

The parties to this Data Processing Addendum ("**Addendum**") agree that Pitney Bowes Limited ("**Service Provider**") provides its Mailstream on Demand product to you (the "**Client**") pursuant to an underlying agreement (the "**Agreement**"). The parties also agree that the Addendum sets forth their obligations with respect to processing Personal Data, as defined herein, carried out by Service Provider in connection with services (the "**Services**") provided to Client pursuant to the Agreement.

1. Definitions

"Applicable Privacy Law(s)" means all applicable laws and regulations relating to the Processing, protection, or privacy of the Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, by way of example only and is not limited to, the European Union General Data Protection Regulation of 2018 and the UK GDPR; and similar laws and regulations, worldwide, all as enacted, amended, superseded, or updated from time to time.

"**Authorized Persons**" means any person who Processes Personal Data on Service Provider's behalf in connection with the Services, including Service Provider's employees, officers, partners, principals, and contractors.

"**Business Purposes**" means the Services described in the Agreement, any other purpose specifically identified in Schedule 1 to this DPA, or any lawful instructions of the Client pursuant to the Agreement and Schedule 1.

"**Data Subject**" means an individual who is the subject of the Personal Data and to whom or about whom the Personal Data relates or identifies, directly or indirectly.

"**Personal Data**" means any information the Service Provider Processes for the Client in connection with the Service that (1) identifies or relates to an individual who can be identified directly or indirectly from the data alone or in combination with other information in the Service Provider's possession or control or that the Service Provider is likely to have access to, or (2) the Applicable Privacy Law otherwise defines as protected "personal data", "personally identifiable information", "personal information", or similar term.

"**Processing, Processes, and Process**" means any activity that involves the use of Personal Data, or as the Applicable Privacy Law may otherwise define the terms processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

"**Security Incident**" means any actual and known unlawful breach of security leading to, the theft, destruction, loss, alteration, unauthorized disclosure or access to any Personal Data, in each case, which would reasonably be expected to have a material adverse effect on Client's business operations or financial condition, including without limitation any incident that rises to the level of a reportable security breach under the Applicable Privacy Law.

"**Sensitive Personal Data**" means (i) Personal Data concerning racial or ethnic origin, citizenship or immigration status, political opinions, religious or philosophical beliefs, or trade union membership; (ii) genetic data; (iii) biometric data when Processed to uniquely identify a natural person; (iv) mental or physical health or condition; (v) sex life or sexual orientation; (vi) criminal convictions and offences or related security measures; (vii) precise geolocation; and (viii) such other subsets of Personal Data that are deemed "sensitive" under Applicable Privacy Laws.

"**Term**" means (a) the term of the Agreement; and (b) any period after the termination or expiry of the Agreement during which the Service Provider Processes Personal Data, until the Service Provider has deleted, destroyed, or returned such Personal Data in accordance with the terms of the Statement of Work, including this DPA.

2. Roles and Scope of Processing

2.1 Service Provider shall Process Personal Data under the Agreement only as a processor acting on behalf of Client.

2.2 Service Provider shall: (i) Process the Personal Data solely for the purposes of providing the Services to Client under the Agreement and in accordance with the Business Purposes; and (ii) not Process Personal Data for its own purposes or those of any third party.

2.3 For the avoidance of doubt, Service Provider shall not: (i) sell, rent, or trade Personal Data; (ii) retain, use, or disclose the Personal Data for any purpose other than for the Business Purposes, including to retain, use or disclose Personal Data for a commercial purpose other than performing its Services under the Agreement; and (iii) retain, use, or disclose the Personal Data outside the direct business relationship between Service Provider and Client.

2.4 The Client retains control of the Personal Data and remains responsible for its compliance obligations under the Applicable Privacy Law(s), including without limitation providing any required notices and obtaining required consents, and for the Processing instructions it gives to the Service Provider. Each Party shall comply with its respective obligations under Applicable Privacy Law(s) in all material respects relating to any Personal Data it Processes under this DPA.

2.5 Schedule 1 describes the general Personal Data categories and Data Subject types the Service Provider may Process to fulfill the Business Purposes.

3. Rights of Data Subjects and Cooperation

3.1 **Cooperation**. Service Provider shall, taking into account the nature of the Processing, reasonably cooperate with Client as necessary to enable Client to:

(a) respond to any valid requests or complaints from Data Subjects and governmental and regulatory or judicial bodies relating to the Processing of Personal Data under the Agreement, including requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws. If any such request, complaint or communication is made directly to Service Provider, it shall promptly notify Client of the same in writing;

(b) to conduct and document data protection assessments, customer

(c) impact assessments, or similar assessments as variously defined, and when required, by Applicable Privacy Laws; and

(d) to document Service Provider's compliance with its obligations under Applicable Privacy Laws.

3.2 **Subpoenas and Court Orders**. If Service Provider receives a valid subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other governmental, regulatory or judicial authorities) seeking the disclosure of Personal Data, Service Provider shall (if permitted by law) promptly notify Client in writing of such request, and, at Client's expense, reasonably cooperate with Client if Client wishes to limit, challenge, or protect against such disclosure, to the extent permitted by applicable laws.

4. Security Measures and Incident Response.

4.1 **Security Measures**.

(a) Service Provider will implement and maintain reasonable technical and organizational security measures in accordance with industry-standard practices for its industry designed to protect from Security Incidents and to preserve the security, integrity and confidentiality of the Personal Data including (but not limited to) in the event of disruption, disaster or failure of Service Provider's primary systems or operational controls ("**Security Measures**"), including the Security Measures set out in Schedule 2 of this DPA. Such Security Measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing, and shall at a minimum, comply with the requirements of Applicable Privacy Laws.

(b) If in connection with the Services, Service Provider or any Authorized Person is granted access to or connects to any computing system, network, platform, facilities, or telecommunications or other information system (the "**Client Systems**") owned, controlled, or operated by or on behalf of Client or any of its affiliates, then Service Provider and any such access or connection to the Client Systems is strictly for the purpose of Service Provider's performance of the Services under and in accordance with the Agreement.

(c) Each Authorized Person will agree in writing to protect the confidentiality and security of Personal Data. Service Provider agrees that Authorized Persons with access to Personal Data are required to protect and Process all Personal Data in a manner consistent with the terms of the Agreement and this DPA.

4.2 **Security Incident Response**. In the event of a Security Incident, Service Provider shall use commercially reasonable efforts to, without undue delay and in any event not later than 72 hours after becoming aware of such Security Incident, inform Client and provide a written summary in reasonable detail of the Security Incident.

4.3 Furthermore, in the event of a Security Incident, Service Provider shall use commercially reasonable efforts to:

(a) provide information required to fulfill Client's data breach reporting obligations under (and in accordance with the timescales required by) Applicable Privacy Laws. Such information may include without limitation:

(i) the nature of the Security Incident including, where possible, the categories and approximate number of Data Subjects concerned and approximate number of data records concerned, in each case relating to Client data or Personal Data;

(ii) the name and contact details of the contact point within Service Provider who can provide more information on the Security Incident; and

(iii) a description of the measures Service Provider will take, proposes to take, or suggests that Client takes to address the Security Incident, including, where appropriate to mitigate its possible adverse effects.

(b) promptly (i) prevent, remedy, or mitigate the effects of the Security Incident, (ii) preserve material records and information related to such activities, and (iii) investigate the nature and scope of the Security Incident; and

(c) cooperate with Client in notifying affected individuals and other parties in accordance with Applicable Privacy Laws.

5. Security Audits.

5.1 Service Provider shall use commercially reasonable efforts to maintain records in accordance with ISO 27001 or similar Information Security Management System ("**ISMS**") standards. Promptly following reasonable written request from Client, Service Provider shall provide copies of relevant external ISMS certifications, audit report summaries, and/or other documentation concerning Service Provider's data systems and centers related to Personal Data. Service Provider shall, no more than once during any 12-month period, also respond to Client's written security questionnaires and meet by teleconference or in person to address any follow-up questions; provided, any such meetings must be conducted during Service Provider's normal business hours and in a manner to minimize disruption to Service Provider's operations.

6. Return or deletion of Personal Data

6.1 **Deletion on Request.** Promptly following Client's written request, Service Provider shall: (a) securely destroy (upon written instructions of Client) or return to Client all Personal Data (including copies) in its possession or control, provided, that this requirement shall not apply to the extent that Service Provider is required by any applicable law to retain some or all of the Personal Data, in which event Service Provider shall isolate and protect the security and confidentiality of such Personal Data and prevent any further Processing except to the extent required by such law and shall destroy or return to Client all other Personal Data; and/or immediately cease Processing all Personal Data; and provided further, Service Provider has no obligation to perform Services to the extent Client's request to destroy or return Personal Data prevents Service Provider from doing so.

7. Special Jurisdictional Provisions

7.1 Service Provider shall promptly notify Client whenever Service Provider determines that it can no longer meet its obligations under any Applicable Privacy Laws.

8. Cross-Border Transfers of Personal Data

8.1 If the Applicable Privacy Laws restrict cross-border Personal Data transfers, the Client will transfer that Personal Data to the Service Provider only under the following conditions:

(a) The Service Provider, either through its location or participation in a valid cross-border transfer mechanism under the Applicable Privacy Laws, may legally receive the Personal Data. The parties shall identify in Schedule 1 of this DPA the location(s) where Service Provider may receive Personal Data and any mechanisms that enable the Service Provider to receive that Personal Data, and shall immediately inform the other of any changes impacting the continued validity of such locations or mechanisms;

(b) The Client obtained valid Data Subject consents to the transfer Personal Data under the Applicable Privacy Laws; or

(c) The transfer otherwise complies with the Applicable Privacy Laws for the reasons set forth in a writing executed by the parties and incorporated into this DPA and/or in Schedule 1.

8.2 The Service Provider will not transfer any Personal Data to another country unless the transfer complies with the Applicable Privacy Laws.

9. Subcontractors

9.1 Client acknowledges and agrees that Service Provider uses subcontractors to provide the Services under the Agreement.

9.2 To the extent that Service Provider's subcontractors Process Personal Data in connection with the Services, Service Provider retains control over such Personal Data and enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA.

9.3 Service Provider maintains a list of subcontractors that Process Personal Data in connection with the Services, which list is available upon Client's request and/or in Schedule 1 of this DPA.

10. Miscellaneous

10.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. This DPA is incorporated into the Agreement. Interpretations and defined terms set forth in the Agreement apply to the interpretation of this DPA. The Schedules form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Schedules.

10.2 If there is any conflict between:

(a) this DPA and the Schedules, this DPA will prevail as to that conflict;

(b) this DPA and the Agreement, this DPA shall prevail as to that conflict; and

(c) this DPA and/or the Agreement on the one hand, and any executed Standard Contractual Clauses and/or Applicable Privacy Laws on the other hand, the Standard Contractual Clauses and/or Applicable Privacy Laws, as the case may be, will prevail as to that conflict.

10.3 The obligations placed upon the Service Provider under this DPA shall survive for the Term.

10.4 This DPA may not be modified except by a subsequent written instrument signed by both parties.

10.5 The parties agree that this DPA shall replace any existing data Processing (or equivalent) agreement the parties may have previously entered into in connection with the Services.

10.6 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Privacy Laws.

10.7 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

SCHEDULE 1

Personal Data Processing Purposes and Details

A. LIST OF PARTIES

Name: As set out in the Agreement
Address: As set out in the Agreement **Contact person's name, position and contact details**: As set out in the Agreement
Activities relevant to the data transferred under Module 2 of the SCCs: as described in the Agreement.
Role: Controller or Processor

Name: Pitney Bowes Limited
Business Address: Langlands House, 130 Sandringham Avenue, Harlow, CM19 5QA, United Kingdom
Contact person's position and contact details: Associate General Counsel, privacyoffice@pb.com
Activities relevant to the data transferred under Module 2 of the SCCs: as described in the Agreement.
Role: Processor

B. DESCRIPTION OF THE TRANSFER AND PROCESSING

Categories of Data Subjects: Service Provider will Process Personal Data relating to the following categories of Data Subjects (check all that apply):

[X] employees (Client personnel)
[X] individual independent contractors (individuals acting in a business capacity as independent contractors to Client)
[X vendors' employees (individuals acting in a business capacity who are employees of other vendors, contractors, or suppliers of Client)
[X] consumers or customers (individuals acting in a personal or household capacity who engage with products or services of Client, including visiting a website, creating an account, subscribing to a service, or making a purchase)
[X] job applicants (individuals seeking employment from Client, other than as talent)
[X] other (specify where possible): **[_____]**

Categories of Personal Data: Depending on the contents of the mail provided by Client to Service Provider, Service Provider may Process the following categories of Personal Data (check all that apply):

[X] personal identification (name, date of birth)
[X] government issued identification (driver's license, social security number, or other national identity number)
[X] contact details (email, phone, address)
[_] real-time or precise geolocation
[X] education and training details
[X] employment-related data
[X] family, lifestyle, and social circumstances
[X] financial, economic and insurance data, including financial account numbers
[X] billing and payment information
[_] digital, device and social media identifiers or digital profiles
[X] financial or online service account access credentials
[X] contents of communications not directed to Service Provider or Client
[X] any other categories of Personal Data provided by the Client to Service Provider in connection with the Services (specify where possible): any additional Personal Data contained in mail sent by the Client via the Services.

Service Provider may also Process the following Sensitive Personal Data (check all that apply):

[_] racial or ethnic origin
[_] citizenship or immigration status
[_] political opinions
[_] religious or philosophical beliefs
[_] trade union membership
[_] precise geolocation
[_] genetic data
[_] biometric data

[X] mental or physical health
[_] sex life or sexual orientation
[X] criminal convictions or offences or related security measures
[X] any other categories of Sensitive Personal Data provided by the Client to Service Provider in connection with the Services

Frequency of Transfer: Service Provider will engage in transfers of Personal Data with the following frequency:
[_] "One-off" (Personal Data will be transferred only on seldom, ad hoc basis.)
[_] Occasional (Personal Data will be transferred intermittently, but on a more predictable or frequent basis than ad hoc.)
[X] Ongoing/regular (Personal Data will be transferred on an ongoing or regular basis, not intermittent.)

Business Purposes for Processing (subject matter, nature, and purpose of the Processing operations): Service Provider will Process Personal Data for the purpose of providing the Services, and for such other purposes as may be described in the Agreement or written instructions of Client.

Duration of Processing (the period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period): Service Provider will Process the Personal Data only for as long as Services are provided under the Agreement.

Subcontracting: Service Provider has engaged the subcontractors listed below for Processing as of the date of the A, and maintains that list which is available on Client's request:

Name of Sub-processor	**Location**	**Purpose**
Amazon Web Services	Paris, France	Cloud hosting and infrastructure provider
Pitney Bowes India	New Dehli, India	Any necessary third line support
Paragon Customer Communications (London) Limited	UK	Print services
A. Mclay and Company Limited	UK	Print services
Solution Dynamics (International) Limited	UK	Software system provider

C. CROSS-BORDER TRANSFERS

a. UK International Data Transfer Agreement ("IDTA") and UK International Data Transfer Addendum ("UK Addendum"). If applicable, the parties agree that the IDTA and the UK Addendum will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the IDTA and the UK Addendum, the IDTA and the UK Addendum will be deemed entered into by both parties (and incorporated into this Addendum by this reference).

b. 2021 Standard Contractual Clauses. If applicable, the parties agree that the 2021 SCCs will apply to Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA that are subject to the 2021 SCCs, the 2021 SCCs will be deemed entered into by both parties (and incorporated into this Addendum by this reference). Where the data exporter and the data importer (as such terms are defined in the SCCs, "Data Exporter" and "Data Importer" respectively) are directed to select a module, the parties acknowledge that:

Module 2 (Controller to Processor) of the 2021 Standard Contractual Clauses will apply where Client acts as a Controller and Data Exporter of Personal data and Service Provider acts as Processor and Data Importer of Personal Data. The parties agree that the following options will apply: • in Clause 7 of the 2021 SCCs, the optional docking clause will not apply;
• in Clause 9(a) of the 2021 SCCs, Option 2 will apply;
• in Clause 11 of the 2021 SCCs, the optional language will not apply;
• in Clause 17 (Option 1), the 2021 SCCs will be governed by Irish law;
• in Clause 18(b) of the 2021 SCCs, disputes will be resolved before the courts of the Republic of Ireland.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES- INCLUDING MEASURES TO ENSURE THE SECURITY OF THE DATA

This Schedule 2 forms part of the DPA, where Service Provider will apply the following technical and organizational measures:

1. Develop, implement, and maintain a comprehensive written information security program that includes appropriate administrative, technical, and physical safeguards and other security measures designed to ensure the security and integrity of Personal Data in accordance with industry standards and the Applicable Privacy Laws.

2. Strong encryption of Personal Data in transit and at rest, as applicable, that meets industry best practices, is robust against cryptanalysis, is not susceptible to interference or unauthorized access, and for which key access is limited to specific authorized individuals with a need to access Personal Data to engage in Processing.

3. Implement any data transfer mechanism as may be necessary for compliance with Applicable Privacy Laws for transfer of Personal Data to other jurisdictions for legitimate business purposes including (a) the performance of the Services as set forth in the Agreement; (b) to provide any technical and customer support, maintenance, and troubleshooting as requested by Client; and (c) to fulfil all other obligations under the Agreement with due observance of all applicable laws and regulations and preservation of the confidentiality of the information.

4. Access restrictions and procedures, including unique user identification, to limit Processing to authorized Service Provider workforce and devices authorized explicitly by Client through proper separation of duties, role-based access, on a need-to-know and least privilege basis.

5. Multi-factor authentication and use of a virtual private network for any remote access to Service Provider systems or Personal Data.

6. Physical security procedures, including the use of monitoring 24 hours /7 days a week, access controls and logs of access, and measures sufficient to prevent physical intrusions to any Service Provider facility where Personal Data is Processed.

7. Secure disposal of equipment and physical and electronic media that contain Personal Data.

8. Ongoing vulnerability identification, management and remediation of systems including applications, databases, and operating systems used by Service Provider to Process Personal Data.

9. Logging and monitoring to include security events, all critical assets that Process Personal Data, and system components that perform security functions for Service Provider's network (e.g., firewalls, IDS/IPS, authentication servers, anti-virus and malware protection) intended to identify actual or attempted access by unauthorized individuals and anomalous behaviour by authenticated users.

10. Monitoring, detecting, and restricting the flows of Personal Data on a multi-layered basis, including but not limited to the use of network segmentation, secure configuration of firewalls, intrusion detection and/or prevention systems, web application firewalls, and denial of service protections.

11. Processes to detect, identify, report, respond to, and resolve security incidents in a timeframe consistent with industry standards and applicable law, including security incident notification as outlined in the Agreement, of any security incident(s) that result in, or which participating party reasonably believes may result in, unauthorized access to, modification of, or disclosure of Personal Data.

12. Data protection program elements, such as technical measures or documented procedures, to address data minimization and limited retention, data quality, and implementation of Data Subject rights, appropriate to the nature of the Processing and Services.

13. Retention policies, schedules and procedures limited retention of Personal Data for the period necessary to fulfil the purposes outlined in the Agreement, unless a longer retention period is required or allowed by law; or to otherwise fulfil a legal obligation.

14. Appropriate IT governance processes that address risk management, system configuration, and process assurance, including regular and periodic testing and evaluation of the sufficiency of Service Provider's data protection program and technical controls.
15. Business continuity and disaster recovery plans intended to ensure integrity, resiliency, and availability of Service Provider systems and Personal Data, as well as timely restoration of access to Personal Data.