Data Processing Addendum

For Smart Access Management

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

1. Definitions

For purposes of this Addendum, the following terms will have the following meanings:

a. "Controller" means a person or entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

b. "Data Protection Law" means any federal, state, provincial, local, municipal, foreign, European, international, multinational or other law, statute, treaty, rule, regulation, ordinance, code, and guidance issued by regulatory authorities competent to interpret or enforce the same, relating to processing Personal Data, privacy, data protection (the protection of Personal Data), or cybersecurity, as may be amended from time to time;

c. "Data Subject" means the individual to whom Personal Data relates;

d. "Data Subject Request" means a request by a Data Subject for information, access, rectification, erasure, restriction, portability, objection, do-not-sell, deletion, and any other similar requests;

e. "Personal Data" means any information relating to an identified or identifiable natural person including any information defined as "personally identifiable information" or "personal information," or similar terms as such terms are defined under applicable Data Protection Laws, limited to Personal Data that Pitney Bowes Processes in connection with the provision of Services to Customer;

f. "Process" or "Processing" means any operation or set of operations performed upon Personal Data, whether or not by automated means, including the collection, recording, organization, structuring, storage, adaption or alteration, consultation, use, disclosure by transmission, transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

g. "Processor" means a person or entity which Processes Personal Data on behalf of the Controller;

h. "Security Incident" means: (i) any unauthorized acquisition of, access to, or use of Personal Data; or (ii) any breach of security leading to any unauthorized acquisition of, access to, or use of Personal Data ;

i. "Sensitive Personal Data" means (i) Personal Data revealing racial or ethnic origin, 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) data concerning health (v) data concerning a natural person's sex life or sexual orientation; (vi) Personal Data relating to criminal convictions and offences or related security measures and (vii) such subsets of Personal Data that are deemed "sensitive" under

applicable Data Protection Laws;

j. "Standard Contractual Clauses" or "SCCs" means the 2021 Standard Contractual Clauses approved by the European Commission in Decision 914/2021/EU. The SCCs are incorporated into this Addendum;

k. "Sub-processor" means a person or entity which Processes Personal Data on behalf of a Processor; and

l. "Supervisory Authority" means the data protection authority in the applicable Member State of the European Union and the equivalent authorities in each other state within the European Economic Area ("EEA"), Switzerland, the United Kingdom or any other jurisdiction whose Data Protection Laws apply to the Processing of the Personal Data subject to this Addendum.

2. Roles of the Parties

a. With respect to Personal Data Processed by Pitney Bowes in connection with the Services, the parties acknowledge and agree that:

(i) Customer will be a Controller and Pitney Bowes will be a Processor.

(ii) Customer will disclose Personal Data to Pitney Bowes for the specific purposes outlined in the Agreement and as otherwise necessary for Pitney Bowes to provide the Services to Customer.

(iii) The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, for the processing instructions it gives to Pitney Bowes and the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of Personal Data to Pitney Bowes and/or lawful collection of the Personal Data by Pitney Bowes on behalf of the Customer for the duration and purposes of this agreement.

(iv) Schedule 1 of this Addendum (Details of Processing) further specifies a list of the parties, a description of the personal data transfers, and the identity of the competent supervisory authority.

Pitney Bowes Obligations

a. Compliance. Pitney Bowes will comply with all applicable Data Protection Laws and provide the level of privacy protections required by such laws.

b. Security. Pitney Bowes will implement and maintain technical and organizational security measures to adequately protect Personal Data against Security Incidents. Pitney Bowes security measures will include any technical and organizational measures specified in the Agreement and in Schedule 2 to this Addendum.

c. Use Restriction. Pitney Bowes will not: (i) sell Personal Data or otherwise disclose it in exchange for monetary or other valuable consideration, or (ii) Process Personal Data for any purpose other than the purpose of performing the Services or pursuant to the directions of Customer.

d. Data Subject Requests. Pitney Bowes will promptly notify Customer of any Data Subject Requests or communication from Data Subjects relating to the Personal Data it Processes in connection with the Services, without responding to the individual except to acknowledge receipt of the Data Subject Request or communication (unless otherwise required by Data Protection Law or instructed by Customer). Pitney Bowes will assist Customer to effectively allow it to respond to Data Subject Requests, including provision of appropriate technical and organizational measures, and any necessary product features and

functionality. Pitney Bowes will provide such assistance promptly, and in any event within ten (10) business days, of the Data Subject's request or Customer's request for assistance.

e. Governmental Requests. Pitney Bowes will promptly notify Customer of any notices, requests for information, or orders received from governmental or data protection authorities in relation to the Personal Data or Pitney Bowes's Processing of such Personal Data, unless prohibited by law. Pitney Bowes will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. Pitney Bowes will work at the direction of Customer to respond (or promptly provide reasonable assistance for Customer to respond) to such notices, requests for information, or orders from governmental or data protection authorities. If Pitney Bowes is legally obligated to respond to such a request without prior notice to Customer, Pitney Bowes will promptly notify Customer thereafter and provide it with a copy of the request and Pitney Bowes's response, unless legally prohibited from doing so. If Customer informs Pitney Bowes in writing that it may proceed with the disclosure, Pitney Bowes will take steps to ensure that it only discloses the information, including Personal Data, that is legally required to fulfill the request.

f. Personnel Confidentiality. Pitney Bowes will ensure that each of its personnel are subject confidentiality obligations that apply to Personal Data.

g. Audit and Assistance. At Customer's expense, Pitney Bowes will provide and make available to Customer such information and assistance as may be reasonably required to confirm Pitney Bowes's compliance with this Addendum. Pitney Bowes will provide such assistance as reasonably necessary for Customer to comply with Data Protection Law relevant to the Personal Data provided to Pitney Bowes by Customer under the Agreement. Customer will give reasonable advance notice and will conduct any such audit during regular business hours without unreasonably disrupting Pitney Bowes's operations. This provision will not require Pitney Bowes to provide Customer with access to the confidential information of Pitney Bowes's other customers.

h. Security Incidents. Pitney Bowes will promptly, and no later than seventy-two (72) hours after discovery, inform Customer of any actual or reasonably suspected Security Incident. At Customer's direction, Pitney Bowes will provide all information and assistance reasonably required by Customer in order for Customer to investigate, mitigate, and respond to a security incident pursuant to Customer's obligations under any applicable Data Protection Laws, including at minimum, any information or assistance required by applicable Data Protection Law or necessary for Customer to make any notifications of the Security Incident.

i. Sub-processing. If Pitney Bowes subcontracts or assigns any of Pitney Bowes's obligations with respect to the Processing of Personal Data to a Sub-processor, Pitney Bowes will (i) ensure that each Sub-processor has entered into a written agreement imposing obligations no less protective than those included in this Addendum; (ii) perform appropriate due diligence to reasonably determine that each Sub-processor can perform as necessary for Pitney Bowes to meet its obligations under this Addendum; and (iii) remain fully liable for the performance of each Sub-processor. Customer authorizes Pitney Bowes to engage the Sub-processors identified in Schedule 1 to Process Personal Data.

j. Disposal and/or Return. Upon request by Customer at termination or expiration of the Agreement, Pitney Bowes will in accordance with Customer's instructions: (i) return to Customer a copy of the Personal Data in Pitney Bowes's possession in connection with the Agreement, in a form and format reasonably agreed upon by the Parties; and/or (ii) securely dispose of the Personal Data (including all copies) in Pitney Bowes's possession in connection with the Agreement.

(v) Cross Border Data Transfer Mechanisms

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 Customer acts as a Controller and Data Exporter of Personal data and Pitney Bowes 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.

(vi) Interpretation and Order of Precedence

a. In case of any inconsistency, conflict, or ambiguity among the terms the Parties have agreed upon, the documents will govern in the following order: (i) the Standard Contractual Clauses, if applicable; (ii) the Addendum; and (iii) the Agreement. The parties intend for the terms of this Addendum, its appendices, and the Agreement to be construed in the manner that affords the greatest protection to data subjects.

b. For the avoidance of doubt, claims made under this Addendum will be subject to any limitation of liability terms contained in the Agreement and indemnification obligations in the Agreement.

(vii) Term

The term of this Addendum will be concurrent with the Agreement.

(viii) Governing Law

Unless otherwise required by the Standard Contractual Clauses or other data transfer requirements, this Addendum will be subject to the governing law, and subject to the jurisdiction's provisions, identified in the Agreement without giving effect to conflict of laws principles.

SCHEDULE 1

DETAILS OF PROCESSING

This Schedule 1 forms part of the Addendum and also serves as Annex I to Module 2 of the SCCs.

A. LIST OF PARTIES

Data Exporter

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

Data Importer

Name: Pitney Bowes Limited

Address: Langlands House, 130 Sandringham Avenue, Harlow, CM19 5QA, United Kingdom

Contact person's name, position and contact details: Victoria Biswell, 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

a. Categories of Data Subjects: Pitney Bowes will Process Personal Data relating to the following categories of Data Subjects (check all that apply):

[x] employees (personnel engaged by Customer)
[x] contractors (individuals acting in a business capacity as independent contractors to Customer)
[ ] Customer employees/contractors (individuals acting in a business capacity who are employees of other contractors, or suppliers of Customer)
[x] consumers or customers (individuals acting in a personal or household capacity who engage with products or services of Customer, including visiting a website, creating an account, subscribing to a service, or making a purchase)
[X] talent (individuals acting in a professional capacity seeking a role in a production)
[X] job applicants (individuals seeking employment from Customer, other than as talent)
[x] other (specify where possible): any person who access the premises of the Customer

b. Categories of Personal Data: Pitney Bowes will 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 location
[x] education and training details
[x] employment-related data
[_] family, lifestyle, and social circumstances
[x] financial, economic and insurance data, including financial account numbers
[_] billing and payment information
[_] digital, device and social media identifiers or digital profiles
[_] account credentials
[_] contents of communications not directed to Pitney Bowes or Customer
[_] any other categories of Personal Data provided by the Customer to Pitney Bowes in connection with the Services (specify where possible):

Pitney Bowes may also Process the following Sensitive Personal Data (check all that apply):

[_] racial or ethnic origin
[_] political opinions
[_] religious or philosophical beliefs
[_] trade union membership
[_] genetic data
[X] biometric data
[X] data concerning health
[_] sex life or sexual orientation

c. Frequency of Transfer: Pitney Bowes 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.)

d. Subject matter, nature and purpose of the Processing operations: Pitney Bowes will Process Personal Data for the purpose of providing the Services, and for such other purposes as may be described in the Agreement or instructions of Customer.

e. 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): Pitney Bowes will Process the Personal Data only for as long as Services are provided under the Agreement.

Subcontracting: Pitney Bowes has engaged the following Sub-processors for Processing as of the date of the Addendum:

Name of Sub-processor	Address and Country of Jurisdiction	Brief Description of Processing activities
Pitney Bowes Inc	3001 Summer Street, Stamford, Connecticut 06926, USA	To provide third line support.
Pitney Bowes India	D-7/3 Okhla Industrial Estate, Phase II, New Dehli, 110020, India	To provide third line support

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority in accordance with Clause 13 of the SCCs shall be *Ireland*.

SCHEDULE 2

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

Pitney Bowes 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 in order 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 underlying agreement; (b) to provide any technical and customer support, maintenance, and troubleshooting as requested by Data Exporter, and (c) to fulfil all other obligations under the underlying 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 Data Importer workforce and devices authorized explicitly by Data Importer 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 Data Importer 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 Data Importer 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 Data Importer 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 Data Importer'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 underlying 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 Data Importer's data protection program and technical controls.

15. Business continuity and disaster recovery plans intended to ensure integrity, resiliency, and availability of Data Importer systems and personal data, as well as timely restoration of access to personal data.