STANDARD CONTRACTUAL CLAUSES

These controller-to-processor Standard Contractual Clauses Addendum to the PoliteMail Terms and Conditions Agreement are entered into on and is effective this [DD/MM/YYYY] by and between [Customer Legal Name] with offices in [Customer Headquarters Address] on behalf of itself and its Affiliates ("Data exporter") and Bootstrap Software Partners LLC (d/b/a PoliteMail Software) with offices in 655 Portsmouth Avenue, Suite 11, Greenland NH 03840 ("Data importer") identified in Clause 1(b) and Annex I.A. Data exporter and Data importer are, at times, jointly referred to as the "Parties".

BACKGROUND

(i) The Parties have entered into an agreement whereby Data importer provides Services (as defined in the Master Subscription License Agreement (the "Agreement")) to Data exporter and/or an Affiliate;

(ii) In connection with the Services, Data importer processes, on Data exporter's and/or an Affiliate's behalf, Personal Data concerning Data exporter's and/or an Affiliate's employees;

(iii) Under the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council) ("GDPR"), Data importer is a Processor, and Data exporter is the Controller;

(iv) Under to Article 28 of the GDPR, Data exporter seeks to obtain written assurances from Data importer that it is processing Personal Data in accordance with the requirements of the GDPR and ensuring the protection of the rights of Data Subjects;

NOW THEREFORE, for good and valuable consideration, the adequacy and sufficiency of which hereby are acknowledged, the Parties agree as follows.

Definitions

"Affiliate" means an entity controlling, controlled by or under common control with Company; and control means the ability, directly or indirectly, to direct the affairs of another by means of ownership, contract, or otherwise.

"Data exporter" means the entity named above, or its relevant Affiliate as the case may be, for whom Data importer provides Services.

"Controller", "Processor", "Processing", and "Supervisory Authority" have the same meanings as in Article 4 of the GDPR.

"Data Subject" means the subject of Personal Data.

"Personal Data" means any information received by Service Provider from, or created or received by Data importer on behalf of, Data exporter, 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 identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person.

"Personal Data Breach" means a suspected or actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to,

Personal Data transmitted, stored or otherwise Processed when that Personal Data is in the possession of Data importer or its agents or subcontractors;

"Required By Law" means that a statute, regulation, court order, or legal process, enforceable in a court of law, mandates the conduct.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the

data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer

in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the

data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

Data exporter may request return or destruction of personal data, in accordance with the terms set forth above at any time in its discretion. Data importer agrees that its destruction of personal data shall be done securely and in a manner that results in the permanent deletion or destruction of the personal data.

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach to [Data Exporter/Controller breach notification address]. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and personal data records concerned), its likely consequences, and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(i) The notification required pursuant to Section 8.6(c), above, shall be provided in writing and no later than 24 hours after data importer becomes aware of the personal data breach.

(ii) In addition to the information described in Section 8.6(c), above, the notice to data exporter of the personal data breach shall include: (A) the date the breach occurred and the date the data importer became aware of the breach; and (B) an identification of any law enforcement agency or supervisory authority that data importer has contacted about the personal data breach and contact information for the relevant official.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

(i) The data importer will promptly reimburse data exporter for all imputed and out-of-pocket costs reasonably incurred by data exporter in connection with the breach, including, but not limited to, costs related to data exporter's provision of notice of personal data breach and to any services offered in a personal data breach notification to affected data subjects.

(ii) In addition to any insurance requirements in the underlying services agreement, data importer shall maintain cyber liability insurance with a limit of five million dollars ($5,000,000) per claim and in the aggregate per calendar year, including coverage for costs arising from or relating to a personal data breach involving personal data in the possession, custody or control of data importer of its sub-processors.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(e) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(f) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(g) the onward transfer is necessary for the establishment, exercise or defense of legal

claims in the context of specific administrative, regulatory or judicial proceedings; or

(h) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(i) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(j) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(k) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(l) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(m) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

9.1 The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least sixty days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2 Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.1 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which

[1] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

the data importer is subject pursuant to these Clauses.

9.3 The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4 The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

9.5 The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints (privacyofficer@politemail.com). It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(i) In addition, data importer shall be liable to data exporter for any damages resulting from a personal data breach involving personal data received from data exporter and that was in the possession, custody, or control of data importer or its sub-processors at the time of the breach.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the [Republic of Ireland].

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the [Republic of Ireland].

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

[DATA EXPORTER LEGAL NAME]

By: _____

Name: […]

Title: […]

BOOTSTRAP SOFTWARE PARTNERS LLC

By: 

Name: Michael DesRochers

Title: Managing Director, Chief Privacy Officer

APPENDICES

ANNEX I

A. LIST OF PARTIES

B. DESCRIPTION OF TRANSFER

C. COMPETENT SUPERVISORY AUTHORITY

ANNEX II

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

ANNEX III

LIST OF SUBPROCESSORS

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name:

   Address:

   Contact person's name, position and contact details:

   Activities relevant to the data transferred under these Clauses: Managing a software for e-mail communications

   Signature and date: _____

   Role: Controller

2. Affiliates

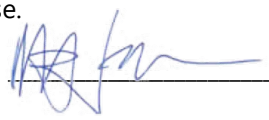
Data importer(s):

1. Name: Bootstrap Software Partners LLC (d/b/a PoliteMail Software)

   Address: 300 Constitution Avenue, Suite 200, Portsmouth NH 03801

   Contact person's name, position and contact details: Michael DesRochers, Managing Director, michael.desrochers@politemail.com, Managing Director Chief Privacy Officer (603) 294-4191

   Activities relevant to the data transferred under these Clauses: Responsible for data security across customer base.

   Signature and date: 

   Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees, contractors and temporary workers (current, former, prospective) of data exporter;

Data exporter's employees (current, prospective, former);, contractors or temporary workers of legal entity collaborators/contact persons (natural persons);

Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter who use the Services and/or receive email communications of the data exporter;

Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of or mentioned in documents or correspondence from or to the data exporter).

Categories of personal data transferred

Personal Identifiers of email senders and recipients including: name, email address and IP address, and other related data including working hours, time zone, language preference and manager which are generally related to a Microsoft email address account.

Data Processor will process and store data and meta data regarding the email messages including:

- From Address, reply-to address
- To/recipient email addresses (and any related distribution list names, as a member of)
- Subject line
- Time and Date of email sent
- Number of words and images within the email content
- Location of images within the email
- URLs contained within the email
- Any images or files uploaded by the user of the Services to include within the email message

Data Processor will also process and store employee (i.e., recipient) interactions with the email, including:

- https request for encoded images (to measure email open page views and page view durations);
- https requests for encoded URLs (to measure link clicks);
- data contained in https headers and requests including IP addresses and related geo-location of such network data, user agent strings including browser, OS, and device identifiers;
- authentication data and tokens in regards to authorized system and services access.

Data Controller may elect to include (using the tools and functionality of the Services) other employee or HR data and personal data imported from other sources, such as, but not necessarily limited to or including:

- Employee ID, employment status, region, business unit, management level, benefits participation

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis.

Nature of the processing

Processing internal email communications, including statistical interaction analytics and the collecting, organizing, and storing distribution lists including names and company email addresses (personal data) of Controller's employees.

Purpose(s) of the data transfer and further processing

To process Personal Data only (a) to provide Controller the Services in accordance with Controller's documented instructions, and (b) for PoliteMail's legitimate business operations.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained for the term of the Agreement. During the Term the Controller may export the data using the tools provided, or request an extract of the data. Data shall be retained for 30 days after expiration or termination of Controller's subscription. After the 30-day retention period ends, PProcessor shall permanently destroy and delete the Personal Data, including backups of such data within an additional 30 days, unless PoliteMail is permitted or required by applicable law.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

All data will be processed by Microsoft Azure as cloud hosting sub processor for Term of agreement. Note sub processor is not provided with data access, but does control hardware and network.

Sub-processing transfers involve security monitoring of log files, SQL systems performance monitoring, and associated SQL database maintenance (e.g. profiling and analysis of database transactions, rebuilding of indexes, creation of indexes, and investigation into data anomalies as required).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in the EU, the supervisory authority in the country of the establishment of the data exporter. A full list of EU supervisory authorities can be found here https://edpb.europa.eu/about-edpb/about-edpb/members_en. In any other cases the supervisory authority is the authority competent in the [Republic of Ireland].

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES
INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO
ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

I. TECHNICAL AND ORGANIZATIONAL MEASURES

A. Information Security Governance

Data importer shall protect Customer Data, Confidential Information including Personally Identifiable Information through implementation and maintenance of policies and controls in alignment with the most recent versions of the international standard ISO27001 and 27002.

Data importer maintains security documentation describing its security measures and the relevant procedures in detail, as well as routine assessment and review documentation, and makes such available to data controller upon request.

Data importer has established a Chief Security officer with overall responsibility for information security governance and a peronnel structure and responsibilities for information security systems and procedures. Data importer has established a Chief Privacy officer for privacy governance. Roles and responsibilities have been formally defined for all members of the information security and privacy teams and have been documented.

Data importer maintains an inventory of all data storage media on which Customer Data is stored.

B. Administrative Access Controls

1. Access Authorization And Workforce Clearance: An employee or contractor will be authorized to access personal data ("Authorized Users") only if the individual is deemed trustworthy based upon prior service to the data importer or the successful completion of a background check where permitted by applicable law. Data importer permits Authorized Users to access personal data only on a need-to-know basis and only as necessary to perform assigned job responsibilities.

2. Confidentiality Agreement: Before establishing access for an Authorized User, data importer requires that the Authorized User execute a confidentiality agreement that applies to the personal data or otherwise acknowledges an obligation of confidentiality.

3. Access Establishment: Data importer separates functions between those authorized to assign access rights and those authorized to establish access to data importer's information systems.

4. Review Of Access Rights: On at least a quarterly basis and when an Authorized User changes positions, data importer reviews and, if necessary, revises or terminated the Authorized User's rights of access to workstations, programs and processes to limit the Authorized User's access to personal data to the minimum necessary to perform assigned job functions. Data importer will delete any personal data stored on the Authorized User's computer that no longer is needed by the Authorized User in his or her new position.

5. Denial Of Access To Terminated Authorized Users: Upon termination of any Authorized User's relationship with data importer, data importer promptly does the following: (a0 terminate the Authorized User's rights to access personal data and obtain the return of any devices (such as tokens or key cards) used to obtain access to personal data; (b) obtain the return of all keys, key cards, and other devices that permit access to physical locations containing personal data in paper form; (c) ensure that the terminated Authorized User does not have unescorted access to areas containing personal data in paper form; (d) ensure that all personal data is removed from any computer equipment used by the terminated Authorized User before re-issuing that equipment to another Authorized User.

C. Training

Data importer provides (a) initial training to relevant personnel on how to implement and comply with its information security program, including identifying and reporting a personal data breach, and (b) periodic refresher training and security awareness reminders. Data importer permits newly hired Authorized Users to access personal data only after completion of the initial data security training.

D. Security Incident Response

Data importer has created a security incident response team (SIRT) with assigned roles and responsibilities. Data importer has implemented procedures for identifying security incidents, including personal data breaches, and a plan for responding to security incidents. Data importer periodically tests the security incident response plan. Data importer has established a mechanism for employees to report security incidents, including suspected and actual personal data breaches. Data importer requires all employees to immediately report the loss, theft, or otherwise of any equipment on which personal data is stored.

E. Third Party SubProcessors

Data Importer has a third party risk assessment and security agreement review process performed prior to engaging with third parties, and prior to any subprocessing of Customer Data or such third parties involvement in providing the Services.

II. TECHNICAL MEASURES

A. Evaluation And Monitoring

1. Risk Assessment: Data importer annually conducts an assessment of the potential risks and vulnerabilities to the systems andconfidentiality, integrity and availability of personal data.

2. Security Policies And Procedures: Data importer routinely reviews, evaluates and updates and implementes policies and procedures to reduce risks and vulnerabilities to a reasonable and appropriate level to protect the confidentiality, integrity and availability of personal data and to prevent accidental or unauthorized use, disclosure, alteration, loss or destruction.

3. System Activity Monitoring

1. Logging: Data importer has (a) enabled logging on computer systems that store personal data; (b) implemented a process for the review of exception reports and/or logs, and (c) developed and documented procedures for the retention of monitoring data.

2. Monitoring: Data importer periodically reviews information system activity records — including audit logs, access reports, privileged operations, error logs on servers, and security incident

tracking reports, and changes to systems security — to ensure that implemented security controls are effective and that personal data has not been potentially compromised. Monitoring includes (a) reviewing changes affecting systems handling authentication, authorization, and auditing; (b) reviewing privileged access to production systems processing personal data; and (c) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

3. Risk Assessments: Data importer periodically conducts, and engaged third parties to conduct, assessments, reviews and reports on compliance with security policies and procedures. Data importer performs monthly security scans of both its internal network and servers as well as production (cloud) network and servers. Data importer performs static and dynamic scans of its software products and standard systems configurations prior to each major version release. Data importer engages a third party, at least annually, to perform an independent assessment of the information security program as well as a third party penetration test of its production systems. Data importer will make such third-party assessment reports available to data exporter upon request.

C. Protections Against Malicious Actors

1. Network and Host Security: Data importer employs intrusion detection at the network level and maintains an up-to-date host-based firewalls and access control lists (ACLs). Data importer engages in security patch management to ensure that security patches are installed as soon as is reasonably practicable.

2. Anti-Malware Protection: Data importer ensures that protections against malicious software (e.g., anti-virus protection, spyware detection software, etc.) are installed before computers and other devices are connected to any of data importer's networked systems. The software is kept current.

D. Technical Access Controls

1. Unique User ID/Secure Passwords: All Authorized Users will be assigned a unique user ID and will be required to create a strong/complex password, or to use a biometric identifier, to access data importer's network. Systems requiring entry of a password suppress, mask or otherwise obscure the password so that it cannot be viewed by an unauthorized person. All passwords are encrypted while in storage. Authorized Users are required to change passwords on a regular basis. Authorized Users are prohibited form sharing passwords with any other person.

2. Access Restrictions: Data importer has implemented technical controls so that each Authorized User will be able to gain access only to those categories of personal data to which access is necessary to perform assigned job responsibilities.

3. Encryption: Data importer encrypts personal data in transit, using Transport Layer Security (TLS) encryption. Data importer encrypts personal data at rest using 256-bit AES encryption or stronger. Mobile devices and portable electronic storage media used to store personal data must be encrypted.

4. Remote Access: Data importer permits remote access to its networks only via secured, authenticated connections utilizing a Virtual Private Network ("VPN") plus IP restrictions and MFA.

5. Secure Disposal: Data importer has established procedures for the secure and permanent destruction of personal data stored in paper and electronic form.

E. Contingency Planning

1. Back-Ups: Data importer backs up personal data on a regular schedule (daily incremental, weekly full). Back-ups are encrypted and stored in a using zone redundant, cloud storage apart from the primary storage. PoliteMail's redundant backup storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed. Restoration processes are tested within 60 days systems deployment, and at least annually.

2. Protection from Disruptions. Data importer uses various systems and monitoring processes and equipment to protect against loss of data due to power supply failure, line interference or other network interruptions.

3. Business Continuity/Disaster Recovery: Data importer maintains contingency and emergency and plans for the systems and facilities which process Customer Data.

- Data importer has developed and maintains a business continuity/disaster recovery plan to ensure that data importer can promptly resume service and restore data exporter's access to personal data in the event of a physical or technical incident occurrence (for example, fire, ransomware attack, vandalism, system failure, pandemic flu, and natural disaster).

F. Change and Configuration Management

Data importer maintains policies and procedures for managing changes to production systems, applications, and databases processing personal data and for documenting the changes.

G. Data Disposal. Data importer uses NIST-800 processes to delete Customer Data when it is no longer needed. For cloud services production systems, this is by permanent destruction of encryption keys and logical disposal of cloud storage drives (NIST 800-88).

H. Incident Response Process

Data importer tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.

Data importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

For each security breach that is a Security Incident, notification by data importer (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 24 hours of evidence of breach.

III. PHYSICAL SAFEGUARDS

1. Data importer limits physical and logical access to facilities and systems where data is processed or stored to identified, authorized individuals. Data importer's facilities where personal data are physically secured against unauthorized access by, for example, keys, access cards, and/or security guards. Guests and service providers must register at a reception area and are prohibited from unescorted access to data importer's facility.

2. All servers and network equipment containing personal data are maintained in a location subject to controlled physical access. Only authorized employees may have

unescorted access to secure areas where servers and network equipment are located. Video surveillance cameras monitor secured areas where production servers, data storage and other production network equipment are located.

3. Only authorized employees may have unescorted access to areas with computers and other electronic resources that permit access to personal data. Access is restricted by a proximity card or keyor some similar method. Physical access rights are promptly terminated when an employee no longer needs physical access to areas containing electronic resources that permit access to personal data.

4. Data exporter requires authorized personnel to ensure that all equipment (computers, laptops, etc.) utilized to access to personal data, that are assigned to, or regularly used by, them are maintained and used in a manner consistent with their function and such that the possibility of damage and/or loss is minimized.

5. Except for equipment designed to be portable, such as laptops, computer equipment used to access personal data should not be removed from data importer's premises without prior authorization.

IV. PERSONAL DATA MANAGEMENT

A. Privacy by Design Data Minimization

Data importer has subjected its systems and applications used to process personal data to a review for compliance with privacy-by-design and privacy-default principles and has applied the results of that review to the design of its systems and applications that process personal data. Data importer's systems and applications have been designed to collect, use, disclose, and otherwise process the minimum personal data necessary to provide the services that are the subject of the Parties' underlying Agreement.

Data importer's systems and applications have been programmed to automatically delete personal data in accordance with the underlying Agreement, or data controllers data retention instructions, unless data importer is required by law to retain personal data for a longer period of time.

B. Accountability

Data importer maintains a record of processing activities that complies with GDPR, art. 30, with respect to its processing of personal data received form, or created or received on behalf of, data exporter. Data importer shall make such records available to data exporter upon request.

C. Data Subject Rights

1. Correction/Update Of Personal Data: Data importer provides options through its website to allow data subjects to request correction, updating or removal of their personal data and/or provides multiple methods (e.g., chat bot, webform, e-mail address) by which data subjects may submit requests. Such requests shall be referred to the data controller, and data importer shall assist with any corrections as necessary..

2. Erasure: Data importer has established internal procedures and technical mechanisms to ensure that personal data can be permanently deleted from production systems and back-ups in response to a request from a data subject or data controller, if and to the extent required by GDPR, art. 17.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: Microsoft Azure

   Address: Redmond, Washington

   Contact person's name, position and contact details: NA

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Cloud Services Hosting and cloud data storage.

2. Name: Amazon AWS

   Address: Seattle, Washington

   Contact person's name, position and contact details: NA

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Cloud Services Hosting and cloud data storage (fail over), email whitelisting service (email processing for MX broadcasting).

3. Name: Straight Path SQL, LLC

   Address: PO Box 591 Sanbornville NH 03872

   Contact person's name, position and contact details: Mike Walsh, CEO

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): SQL Server performance monitoring and maintenance services, including profiling, diagnosis, and indexing or reindexing as required.

ADDENDUM TO STANDARD CONTRACTUAL CLAUSES

(UNITED KINGDOM)

1.1 *Part 1: Tables*

1.1.1 *Table 1: Parties*

Start date	The date signed by both parties below.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As described in the signature page to the Standard Contractual Clauses.	As described in the signature page to the Standard Contractual Clauses.
Key Contact	As described in Annex I of the attached Addendum EU SCCs.	As described in Annex I of the attached Addendum EU SCCs.
Signature (if required for the purposes of Section 2)	Please see signature page to the Standard Contractual Clauses.	Please see signature page to the Standard Contractual Clauses.

1.1.2 *Table 2: Selected SCCs, Modules and Selected Clauses*

Addendum EU SCCs	■ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective as of the date signed by both parties below (Module 2: standard contractual clauses for the transfer of personal data to third countries – controller to processor)

1.1.3 *Table 3: Appendix Information*

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Please see Annex I of the attached Addendum EU SCCs.

Annex 1B: Description of Transfer:

Please see Annex I of the attached Addendum EU SCCs.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Please see Annex II of the attached Addendum EU SCCs.

Annex III: List of Sub processors (Modules 2 and 3 only):

This Annex III is not applicable because Clause 9(a), Option 1 (specific authorisation of sub processors) of the attached Addendum EU SCCs was not selected.

1.1.4 *Table 4: Ending this Addendum when the Approved Addendum Changes*

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ■ neither Party

1.2 *Part 2: Mandatory Clauses*

1.2.1 *Entering into this Addendum*

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

1.2.2 *Interpretation of this Addendum*

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

1.2.3 *Hierarchy*

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

1.2.4 *Incorporation of and changes to the EU SCCs*

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of

England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

1.2.5 *Amendments to this Addendum*

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

1.3 Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Data Transfer Impact Assessment

[Ireland to US]

PoliteMail Software hereby warrants it has no reason to believe that the laws and practices in the United States, the third country of destination, which are applicable to the processing of the personal data by PoliteMail as importer from the country of [Ireland] prevent the data importer from fulfilling its obligations to provide an adequate level of protection under the GDPR and EU standard contractual clauses (EU SCC) Article 46 and Clause 14.

While public authorities in the United States may seek lawful data access via legislation including Section 702 FISA, EO 12.333 (and PPD-28), PoliteMail is contractually required to defend the personal data from such lawful access, and to notify the controller who may also seek to defend such. As employee data is not the target of data gathering under Section 702 FISA or EO 12.333 there we believe the probability of the company receiving a surveillance order is extremely low.

All data in transit is made via HTTPS and is protected by appropriate encryption of at least AES-256. While some personal data elements, specially email address, is stored and available in clear text to authorized parties, all data at rest is also adequately encrypted and otherwise protected against unauthorized access.