## DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**Addendum**") is in addition to the BEE Pro Terms of Service entered into between MailUp, Inc. ("**MailUp**") and you ("**Customer**") that incorporates this Addendum by reference (the "**Agreement**"), and governs the Processing of Personal Data by MailUp in providing its service pursuant to the Agreement.

If you would like to complete a countersigned copy of this Addendum for your records, the following are the instructions for completing such a copy:

1. This Addendum consists of two parts: the main body of the Addendum, and Exhibit A (including all Appendices thereof).
2. This Addendum has been pre-signed on behalf of MailUp. The Standard Contractual Clauses in Exhibit A have been pre-signed by MailUp as the data importer.
3. To complete a countersigned copy of this Addendum, you must:
   - Complete the information in the signature box and sign this Addendum below.
   - Complete the information required in Exhibit A of this Addendum as the data exporter.
   - Send the completed and signed Addendum by email to dpa@beepro.com .

## 1.    Definitions

"**Authorized Employee**" means an employee of MailUp who has need to know or otherwise access Personal Data to enable MailUp to perform its obligations under this Addendum or the Agreement.

"**Authorized Individual**" means an Authorized Employee or Authorized Subcontractor.

"**Authorized Subcontractor**" means a third-party subcontractor, agent, reseller, or auditor who has a need to know or otherwise access Personal Data to enable MailUp to perform its obligations under this Addendum or the Agreement and who is either (1) listed at https://beefree.io/sub-processors/ at the time the parties enter into this Addendum or (2) later authorized by Customer to do so under Section 4.2 of this Addendum.

"**Data Subject**" means an identified or identifiable person to whom Personal Data relates.

"**Instructions**" means the directions, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by Customer to MailUp and directing MailUp to Process Personal Data.

"**Personal Data**" means any information relating to Data Subject which MailUp Processes on behalf of Customer other than data which can no longer be attributed to an identified or identifiable natural person, and including, without limitation, the following sensitive personal information: a Data Subject's (i) government-issued identification number (including social security number, driver's license number or state-issued identification number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; (iii) genetic and biometric data or data concerning health; or (iv) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or sexual activity, criminal convictions and offences (including commission of or proceedings for any offense committed or alleged to have been committed), or trade union membership.

"**Personal Data Breach**" means a 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.

"**Privacy Shield Principles**" means the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework.

"**Process**" or "**Processing**" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

"**Services**" shall have the meaning set forth in the Agreement.

"**Standard Contractual Clauses**" means the Agreement executed by and between Customer and MailUp and attached hereto as Exhibit B pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on standard contractual clauses for the transfer of personal data to MailUp established in third countries which do not ensure an adequate level of protection.

"**Supervisory Authority**" means an independent public authority which is established by a member state of the European Union, Iceland, Liechtenstein, or Norway.

## 2. Processing of Data

2.1. The rights and obligations of the Customer with respect to this Processing are described herein. Customer shall, in its use of the Services, at all times Process Personal Data, and provide Instructions for the Processing of Personal Data, in compliance with EU Directive 95/46/EC (the "**Directive**"), and, when effective, the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**" and together, "**Data Protection Laws**")). Customer shall ensure that its Instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Customer's Instructions will not cause MailUp to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to MailUp by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the Instructions it provides to MailUp regarding the Processing of such Personal Data. Customer shall not provide or make available to MailUp any Personal Data in violation of the Agreement or which is otherwise inappropriate for the nature of the Services, and shall indemnify MailUp from all claims and losses in connection therewith.

2.2. MailUp shall Process Personal Data only (i) for the purposes set forth in the Agreement, (ii) in accordance with the terms and conditions set forth in this Addendum and any other documented Instructions provided by Customer, and (iii) in compliance with the Directive, and, when effective, the GDPR. Customer hereby instructs MailUp to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Customer in its use of the Services.

2.3. The subject matter, nature, purpose and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in **Exhibit A** to this Addendum.

2.4. Following completion of the Services, at Customer's choice, MailUp shall delete the Personal Data, except as required to be retained by the laws of the European Union or European Union member states.

## 3. Authorized Employees

3.1. MailUp shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

3.2. MailUp shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with MailUp, any Personal Data except in accordance with their obligations in connection with the Services.

3.3. MailUp shall take commercially reasonable steps to limit access to Personal Data to only Authorized Individuals.

## 4. Authorized Subcontractors

4.1. Customer acknowledges and agrees that MailUp may (1) engage the Authorized Subcontractors listed in **Exhibit C** to this Addendum to access and Process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data.

4.2. A list of MailUp's current Authorized Subcontractors (the "**List**") is available at https://beefree.io/sub-processors/ (such URL may be updated by MailUp from time to time). At least ten (10) days before enabling any third party other than Authorized Subcontractors to access or participate in the Processing of Personal Data, MailUp will add such third party to the List and notify Customer of that update via email. Customer may object to such an engagement in writing within ten (10) days of receipt of the aforementioned notice by Customer.

4.2.1. If Customer reasonably objects to an engagement in accordance with Section 4.2, MailUp shall provide Customer with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If MailUp, in its sole discretion, cannot provide any such alternative(s), or if Customer does not agree to any such alternative(s) if provided, MailUp may terminate this Addendum. Termination shall not relieve Customer of any fees owed to MailUp under the Agreement.

4.2.2. If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by MailUp, that third party will be deemed an Authorized Subcontractor for the purposes of this Addendum.

4.3. MailUp shall ensure that all Authorized Subcontractors have executed confidentiality agreements that prevent them from disclosing or otherwise Processing any Personal Data both during and after their engagement by MailUp.

4.4. MailUp shall, by way of contract or other legal act under European Union or European Union member state law (including without limitation approved codes of conduct and standard contractual clauses), ensure that every Authorized Subcontractor is subject to obligations regarding the Processing of Personal Data that are no less protective than those to which the MailUp is subject under this Addendum.

4.5. MailUp shall be liable to Customer for the acts and omissions of Authorized Subcontractors to the same extent that MailUp would itself be liable under this Addendum had it conducted such acts or omissions.

4.6. If Customer has entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the above authorizations will constitute Customer's prior written consent to the subcontracting by MailUp of the processing of Personal Data if such consent is required under the Standard Contractual Clauses.

## 5. Security of Personal Data

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, MailUp shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.

## 6. Transfers of Personal Data

6.1. Any transfer of Personal Data made subject to this Addendum from member states of the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of these countries shall, to the extent such transfer is subject to such laws and regulations, be undertaken by MailUp through one of the following mechanisms: (a) in accordance with the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework (the "Privacy Shield Principles"), or (b) the Standard Contractual Clauses set forth in **Exhibit B** to this Addendum.

6.2. If transfers are made pursuant to 6.1(a), MailUp self-certifies to, and complies with, the Swiss-U.S. and EU-U.S. Privacy Shield Frameworks, as administered by the U.S. Department of Commerce, and shall maintain such self-certification and compliance with respect to the Processing of Personal Data transferred from member states of the European Union, Iceland, Lichtenstein, Norway, or the United Kingdom (the "EEA") or Switzerland to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of the foregoing countries for the duration of the Agreement.

## 7. Rights of Data Subjects

7.1. MailUp shall, to the extent permitted by law, promptly notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively "**Data Subject Request(s)**"). If MailUp receives a Data Subject Request in relation to Customer's data, MailUp will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request.

7.2. MailUp shall, at the request of the Customer, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without MailUp's assistance and (ii) MailUp is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by MailUp.

## 8. Actions and Access Requests

8.1. MailUp shall, taking into account the nature of the Processing and the information available to MailUp, provide Customer with reasonable cooperation and assistance, where necessary for Customer to comply with its obligations under the GDPR, conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by MailUp.

8.2. MailUp shall, taking into account the nature of the Processing and the information available to MailUp, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by MailUp.

8.3. Upon Customer's request, MailUp shall, no more than once per calendar year, either (i) make available for Customer's review copies of certifications or reports demonstrating MailUp's compliance with prevailing data security standards applicable to the Processing of Customer's Personal Data, or (ii) allow Customer or its authorized representative, upon reasonable notice and at a mutually agreeable date and time, to conduct an audit or inspection of MailUp's data security infrastructure that is sufficient to demonstrate MailUp's compliance with its obligations under this Addendum, provided that Customer shall provide reasonable prior notice of any such request for an audit and such inspection shall not be unreasonably disruptive to MailUp's business. Customer shall be responsible for the costs of any such audits or inspections.

8.4. In the event of a Personal Data Breach, MailUp shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as MailUp in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within MailUp's reasonable control).

8.5. In the event of a Personal Data Breach, MailUp shall, taking into account the nature of the Processing and the information available to MailUp, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.6. The obligations described in Sections 8.5 and 8.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. MailUp's obligation to report or respond to a Personal Data Breach under Sections 8.5 and 8.6 will not be construed as an acknowledgement by MailUp of any fault or liability with respect to the Personal Data Breach.

## 9. Limitation of Liability

The total liability of each of Customer and MailUp (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement.

IN WITNESS WHEREOF, Customer and MailUp have executed this EU Data Processing Addendum, as of the date of the last signature written below.

MailUp (MailUp Inc.)

By:

Name: Massimo Arrigoni

Title: CEO

Customer

By: _____

Name: _____

Title: _____

Date: _____

## EXHIBIT A

### Details of Processing

Nature and Purpose of Processing: *as specified in the Agreement*

Duration of Processing: *Term of the Agreement*

Categories of Data Subjects: *users*

Type of Personal Data: *additional users' name, email, and IP addresses; recipient emails and email content*

<u>EXHIBIT B</u>

### Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to MailUp established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organization:

Address: …………………………………………………………..

Tel.: …………………………………………………………..

fax: …………………………………………………………...

e-mail: …………………………………………………………..

Other information needed to identify the organization: [if needed; otherwise "not applicable"]

(the "**data exporter**")

<center>**And**</center>

Name of the data importing organization: *MailUp, Inc.*

Address: *450 Townsend St., San Francisco, CA 94107, USA*

Tel.: *888.962.4587; e-mail: support@beefree.io*

Other information needed to identify the organization: *not applicable*

(the "**data importer**")

<center>each a "**party**"; together the "**parties**",</center>

**HAVE AGREED** on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

<center>*Clause 1*<br>*Definitions*</center>

For the purposes of the Clauses:

a)    'personal data', 'special categories of data', 'process/processing', 'Customer', 'MailUp', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b)    'the data exporter' means Customer;

c)    'the data importer' means MailUp;

d)    'the sub processor' means any processor engaged by the data importer or by any other sub processor the data importer who agrees to receive from the data importer or from any other sub processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e)   'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data Customer in the Member State in which the data exporter is established;

f)   'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*
*Details of the transfer*

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*
*Third-party beneficiary clause*

1.   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.   The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.   The data subject can enforce against the sub processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.

4.   The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4*
*Obligations of the data exporter*

The data exporter agrees and warrants:
   a)   that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

   b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

   c)   that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

   d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks

presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e) that it will ensure compliance with the security measures;

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g) to forward any notification received from the data importer or any sub processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of sub processing, the processing activity is carried out in accordance with Clause 11 by a sub processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

## Clause 5
### Obligations of the data importer

The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

d) that it will promptly notify the data exporter about:
   i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise
   ii. prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
   iii. any accidental or unauthorized access, and
   iv. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information,

with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h)    that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;

i)    that the processing services by the sub processor will be carried out in accordance with Clause 11;

j)    to send promptly a copy of any sub processor agreement it concludes under the Clauses to the data exporter.

*Clause 6*
*Liability*

1.    The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub processor is entitled to receive compensation from the data exporter for the damage suffered.

2.    If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub processor of its obligations in order to avoid its own liabilities.

3.    If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub processor agrees that the data subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.

*Clause 7*
*Mediation and jurisdiction*

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

a)    to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

b)    to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*
*Cooperation with supervisory authorities*

1.    The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.    The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub processor preventing the conduct of an audit of the data importer, or any sub processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*
*Governing Law*

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10*
*Variation of the contract*

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*
*Sub processing*

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub processor as are imposed on the data importer under the Clauses 1. Where the sub processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub processor's obligations under such agreement.
2.   The prior written contract between the data importer and the sub processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.
3.   The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4.   The data exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*
*Obligation after the termination of personal data processing services*

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the sub processor shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2.   The data importer and the sub processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter**:
Name (written out in full): ………………………………………………………………………………………………………
Position: …………………………………………………………………………………………………………………………………
Address: ……………………………………………………………………………………………………………………………………
Other information necessary in order for the contract to be binding (if any): [if needed; otherwise "not applicable"]:
………………………………………………………………………………………………………………………………………………..

Signature: ………………………………………………………………………………………………………………………………….


**On behalf of the data importer**:
Name (written out in full): *Massimo Arrigoni*
Position: *CEO*
Address: *450 Townsend St., San Francisco, CA 94107, USA*
Other information necessary in order for the contract to be binding (if any): *not applicable*
Signature

# APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

### Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

*Data Exporter is the legal entity that has executed the Standard Contractual Clauses as a Data Exporter.*

### Data importer

The data importer is (please specify briefly activities relevant to the transfer):

*MailUp Inc.  is a software as a service company that provides an email editor at https://beefree.io which is used to design emails.*

### Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

*Additional Users and Users' recipients.*

### Categories of data

The personal data transferred concern the following categories of data (please specify):

*Additional users' name, last name, email and IP address. Recipient emails and email content  No other personal data should be transferred.*

### Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

*No special personal data should be transferred.*

### Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

*[Name, last name, email, and IP address of Additional Users are stored in a database and used in the provisioning of the Additional Users feature. They are also used when sending system communications to them. Recipient emails and email content are stored in a database when the "Send test" feature is used, to allow the feature to work.].*

### Note on Personal Data

*When you use BEE Pro, we may process as Data Processor the following information:*

*•additional users' names, last names, emails, and IP address; For example, when an email marketing agency adds a customer of theirs to the system so that the customer can log in and create, edit, review, etc. emails that are being created for them.*

*•email address and message content that belong to a third party. For example, when you decide to use the 'Send a test' feature to send a test email to a recipient who is not you. .*

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

*The technological infrastructure is subcontracted to Italian parent company MailUp S.p.A. Refer to the corresponding description of the technical and organisational security measures available at* [https://www.mailup.com/gdpr-infrastructure/](https://www.mailup.com/gdpr-infrastructure/)