EU Data Processing Addendum (Processor Form)

This EU Data Processing Addendum ("Addendum") supplements the Master Services Agreement (the "Agreement") entered into by and between

_____("Controller") and Mailbutler GmbH ("Processor"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

1.Definitions

1.1. "Anonymous Data" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person without additional information unavailable to any third party other than Authorized Subcontractors.

1.2. "Authorized Employee" means an employee of Processor who has a need to know or otherwise access Personal Data to enable Processor to perform their obligations under this Addendum or the Agreement.

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

1.4. "Authorized Subcontractor" means a third-party subcontractor, agent, reseller, or auditor who has a need to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement, and who is either (1) listed in the following https://support.mailbutler.io/knowledge-base/list-of-sub-processors/ or (2) authorized by Controller to do so under Section 4.2 of this Addendum.

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

1.6. "Instruction" means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by Controller to Processor and directing Processor to Process Personal Data.

1.7. "Personal Data" means any information relating to Data Subject which Processor Processes on behalf of Controller other than Anonymous Data, and includes Sensitive Personal Information.

1.8. "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.

1.9. "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.

1.10. "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.

1.11. "Sensitive Personal Information" means a Data Subject's (i) government-issued identification number (including social security number, driver's license number or state-issued identification

number) or email address; (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.

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

1.13. "Standard Contractual Clauses" means an agreement that may be executed by and between Controller and Processor 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 processors established in third countries which do not ensure an adequate level of protection.

1.14. "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 Controller with respect to this Processing are described herein. Controller 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")). Controller 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 Controller's instructions will not cause Processor to be in breach of the Data Protection Laws. Controller is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Processor by or on behalf of Controller, (ii) the means by which Controller acquired any such Personal Data, and (iii) the instructions it provides to Processor regarding the Processing of such Personal Data. Controller shall not provide or make available to Processor any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Processor from all claims and losses in connection therewith.

2.2. Processor 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 Controller, and (iii) in compliance with the Directive, and, when effective, the GDPR. Controller hereby instructs Processor to Process Personal Data for the following purposes as part of any Processing initiated by Controller 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 Controller's choice, Processor shall return or 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. Processor shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

3.2. Processor 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 Processor, any Personal Data except in accordance with their obligations in connection with the Services.

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

4. Authorized Subcontractors

4.1. Controller acknowledges and agrees that Processor may (1) engage the Authorized Subcontractors 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 Processor's current Authorized Subcontractors (the "List") is available at https://support.mailbutler.io/knowledge-base/list-of-sub-processors/ (such URL may be updated by Processor 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, Processor will add such third party to the List and Controller can subscribe to updates via email. Controller may object to such an engagement in writing within ten (10) days of receipt of the aforementioned notice by Controller.

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

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

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

4.4. Processor 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 Processor is subject under this Addendum.

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

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, Processor 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 Processor 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.

6.2. If transfers are made pursuant to 6.1(a), Processor 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, 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 the foregoing countries for the duration of the Agreement.

7. Rights of Data Subjects

7.1. Processor shall, to the extent permitted by law, promptly notify Controller upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, restriction of Processing, 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)").

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

8. Actions and Access Requests

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

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

8.3. Processor shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Agreement. Controller shall, with reasonable notice to Processor, have the right to review, audit and copy such records at Processor's offices during regular business hours.

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

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

8.6. In the event of a Personal Data Breach, Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance necessary for Controller 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.

8.7. 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 Controller.

9. Limitation of Liability

9.1. The total liability of each of Controller and Processor (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.

EXHIBIT A
Details of Processing

Nature and Purpose of Processing:
In connection with and for the purpose of the provision of Services to Controller under the Agreement

Duration of Processing:
For the term of the Agreement and up to 1 year after termination or expiration of the Agreement

Categories of Data Subjects:
Controller end-users/customers AND/OR Controller employees

Type of Personal Data:

- Name
- Company Name
- Email address
- Address
- VAT Number
- IP Address
- Message Templates and Snippets
- Notes and Tasks
- Email subject line
- Email address of recipient
- Email server credentials
- Name of recipient
- Notes on an account, invoice or transaction
- Payment information (Credit Card & Paypal)

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

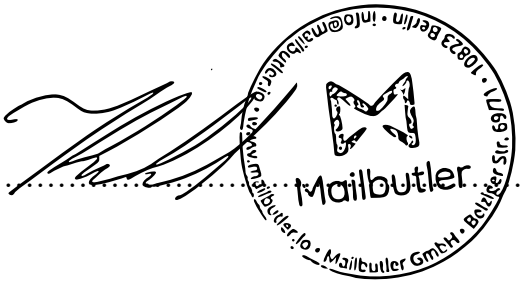
Address: _____

Date Signed: _____

Signature……..……

On behalf of the data importer:

Name (written out in full): Tobias Knobl
Position: CEO Mailbutler GmbH
Address: Belziger Str. 69/71, 10823 Berlin, Germany
Date Signed: April 17th 2018

Signature…… 

……