Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements the Terms of Use ("TOU"), as updated from time to time between you (together with subsidiary(ies) and affiliated entities, collectively, "**Customer**") and MailerLite (together with subsidiary(ies), collectively, "**MailerLite**") (hereinafter collectively referred to as "**Parties**" and individually "**Party**") when the GDPR applies to the Customer's use of MailerLite's Services to process Customer data. If GDPR does not apply to the Customer, Personal Data transferred by the Customer is processed and secured in the same way as described in this DPA.

This DPA is effective from the date the Customer agrees with the terms and conditions of the TOU. If there is any conflict between this DPA and the TOU, the relevant terms of this DPA take precedence.

1. Definitions

1.1. "**Account Data**" means information about the Customer that the Customer provides to MailerLite in connection with the creation or administration of its MailerLite accounts, such as first and last name, user name and email address of an Authorized User or Customer's billing contact. The Customer shall ensure that all Account Data is current and accurate at all times during the term of the TOU.

1.2. "**Authorized User**" means an individual employee, agent or contractor of the Customer for whom subscriptions to Services have been granted pursuant to the terms of the TOU.

Stop War! Help Ukraine!
See what you can do

1.3. "**Customer Credentials**" means access passwords, keys or other credentials used by the Customer in connection with the Services.

1.4. "**Customer Data**" means any Personal Data that MailerLite Processes on behalf of the Customer as a Data Processor in the course of providing its Services.

1.5. "**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

1.6. "**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

1.7. "**Data Protection Laws**" means all data protection and privacy laws and regulations of the EU, EEA and their member states, applicable to the Processing of Personal Data.

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

1.9. "**EEA**" means the European Economic Area, the United Kingdom, and Switzerland.

1.10. "**EU**" means the European Union.

1.11. "**GDPR**" means (a) the Regulation (EU) 2016/679 of the European Parliament and 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 and repealing Directive 95/46/EC (General Data Protection Regulation), and (b) the United Kingdom General Data Protection Regulation.

1.12. "**Personal Data**" means any information relating to an identified or identifiable natural person as defined in the GDPR.

1.13. "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocki
"Process", "Processes" and "Processed" shall be ir

Stop War! Help Ukraine!
See what you can do

1.14. "**Processor**" means a natural or legal person, public authority, agency, or any other body which Processes Personal Data on behalf of the Data Controller.

1.15. "**SCCs**" means the standard contractual clauses as approved by the European Commission.

1.16. "**Services**" means any product or service provided by MailerLite pursuant to MailerLite's TOU.

1.17. "**Sub-Processor**" means any third-party Processor engaged by MailerLite.

1.18. "**UK Addendum**" means the International Data Transfer Addendum to the SCCs (version B1.0) issued by the Information Commissioner's Office under S.119(A) of the UK Data Protection Act 2018, as amended from time to time.

2. Scope and Roles

2.1. MailerLite has agreed to enter into this DPA based on the Customer's belief that Customer Data may include Personal Data that originates from EU/EEA and/or that is otherwise subject to the GDPR. Accordingly, this DPA supplements the TOU and applies exclusively to MailerLite's Processing of Customer Data in providing Services under the TOU to the Customer.

2.2. MailerLite agrees to comply with the following provisions with respect to any Personal Data Processed for the Customer in connection with the provision of the Services.

2.3. The Parties agree that with regard to the Processing of Personal Data, the Customer is the Data Controller and MailerLite is a Data Processor, acting on behalf of the Customer, as further described in **Annex 1** ("*Details of Data Processing*") of this DPA. Each Party will comply with its respective obligations under EU Data Protection Law.

3. Customer's Processing of Personal Data

3.1. The Customer is responsible for the control of Personal Data and must comply with its obligations as a Data Controller un
in particular for justification of any transfer of Cust

Stop War! Help Ukraine!
See what you can do

and its decisions and actions regarding the Processing and use of Personal Data.

3.2. The Customer agrees that it has provided notice and received all consents and rights necessary under Data Protection Laws for MailerLite to Process Customer Data and provide the Services.

4. MailerLite's Processing of Customer Data

4.1. By entering into this DPA, the Customer instructs MailerLite to Process Customer Data to provide the Services in accordance with the features and functionality of the Services.

4.2. In connection with MailerLite's delivery of the Services to the Customer, MailerLite shall Process certain categories and types of the Customer data, only for the purposes described in this DPA and only in accordance with the Customer's documented lawful instructions, including with regard to transfers of Customer data to a third country or an international organization, unless required to do so by EU or Member State of the EU law to which MailerLite is subject. In such a case, MailerLite shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

4.3. The Parties agree that this DPA sets out the Customer's complete and final instructions to MailerLite in relation to the Processing of Customer Data. The Processing outside the scope of these instructions shall require a prior written agreement between Customer and MailerLite. Notwithstanding the foregoing, MailerLite will inform the Customer promptly if it becomes aware that the Customer's instructions may violate applicable EU Data Protection Law.

5. Customer Responsibilities and Restrictions

5.1. Without limiting its responsibilities under the TOU, the Customer is solely responsible for: (a) Account Data, Customer Data and Customer Credentials (including activities conducted with Customer Credentials), subject to MailerLite's Processing obligations under the TOU and this DPA; (b) providing any notices required by EU Data Protection Law to
consents and authorizations required by EU Data P

Stop War! Help Ukraine!
See what you can do

persons whose Personal Data may be included in Account Data, Customer Data or Customer Credentials; and (c) ensuring no Personal Data relating to criminal convictions and offenses (GDPR Article 10) are submitted for Processing by the Services.

6. Security

6.1. 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 Data Subjects, MailerLite shall in relation to Customer Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk (including those outlined in **Annex 2**, "*Security Measures*"). In assessing the appropriate level of security, MailerLite shall take into account the risks that are presented by Processing Customer Data including, in particular, the risks presented by a Customer Data Breach (as defined in Section 10). MailerLite may make such changes to the Security Measures as MailerLite deems necessary or appropriate from time to time, including without limitation to comply with applicable law, but no such changes will reduce the overall level of protection for Customer Data. MailerLite will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-Processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to Process Customer Data have agreed to appropriate obligations of confidentiality.

6.2. The Parties shall take steps to ensure that any natural person acting under the authority of the Customer or MailerLite who has access to Personal Data does not Process them except on instructions from the Customer, unless he or she is required to do so by EU or EU Member State law.

6.3. The Customer is responsible for reviewing the information made available by MailerLite relating to its data security and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations under Data Protection Laws. The Customer acknowledges that MailerLite may update or modify MailerLite's security standards from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

Stop War! Help Ukraine!
See what you can do

6.4. The Customer agrees it is responsible for its secure use of the Services, including securing its Customer Credentials, protecting the security of Customer Data when in transit to and from the Services, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

7. Sub-Processors

7.1. The Customer acknowledges and agrees that MailerLite may engage third-party Sub-Processors in connection with the provision of Services, and hereby consents to MailerLite's use of Sub-Processors. As a condition to permitting a third-party Sub-Processor to Process Customer Data, MailerLite will enter into a written agreement with the Sub-Processor containing data protection obligations no less protective than those in this DPA with respect to Customer Data. MailerLite will restrict its Sub-Processors' access to only what is necessary to maintain the Services or to provide the Services to Customers. Subject to this Section 7, MailerLite reserves the right to engage and substitute Sub-Processors as it deems appropriate, but shall: (a) remain responsible to the Customer for the provision of the Services and (b) be liable for the actions and omissions of its Sub-Processors undertaken in connection with MailerLite's performance of this DPA to the same extent MailerLite would be liable if performing the Services directly.

7.2. Upon the Customer's request by email to legal@mailerlite.com, MailerLite will provide the Customer with a list of then-current third-party Sub-Processors and the nature of the services they provide. The Customer can find an up-to-date list of Sub-Processors in **Annex 4** of this DPA. The Customer may object to any new Sub-Processor on reasonable legal grounds (the "**Objection Notice**") relating to the protection of the Customer Data, in which case MailerLite shall have the right to satisfy the objection through one of the following:

(a) MailerLite will cancel its plans to use the Sub-Processor with regard to Customer Data or will offer an alternative to provide the Services without such Sub-Processor;

(b) MailerLite will take the corrective steps requested by the Customer in its Objection Notice (which removes the Customer's c
use the Sub-Processor with regard to Customer D

Stop War! Help Ukraine!
See what you can do

(c) MailerLite may cease to provide, or the Customer may agree not to use (temporarily or permanently), the particular aspect of the Services that would involve the use of such Sub-Processor with regard to Personal Data, subject to a mutual agreement of the Parties to adjust the remuneration for the Services considering their reduced scope.

7.3. All Objection Notices under Section 7.2 must be submitted by email to MailerLite at legal@mailerlite.com. If none of the options outlined in Clause (a), (b) or (c) of Section 7.2 are reasonably available and Customer's objection has not been resolved to the Parties' mutual satisfaction within 30 days of MailerLite's receipt of the Objection Notice, either Party may terminate the affected Services and MailerLite will refund to the Customer a pro rata share of any unused amounts prepaid by the Customer. The refund will be calculated in proportion to what Services have been provided until the time the Customer has informed MailerLite on terminating the Services. MailerLite does not provide any refunds if the Objection Notice does not have reasonable legal grounds.

8. Data Subject Rights

8.1. If MailerLite receives a request from a Data Subject in relation to the Customer Data then, to the extent legally permissible, MailerLite will advise the Data Subject to submit their request to the Customer and the Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services. The Customer hereby agrees that MailerLite may confirm to a Data Subject that his or her requests relate to the Customer. To the extent the Customer is unable through its use of the Services to address a particular Data Subject request, MailerLite will, upon the Customer's request and taking into account the nature of Customer Data Processed, provide reasonable assistance in addressing the Data Subject request (provided MailerLite is legally permitted to do so and that the Data Subject request was made in accordance with EU Data Protection Law). To the extent permitted by applicable law, the Customer shall be responsible for any costs arising from MailerLite's provision of such assistance.

9. Deletion Upon Expiration

9.1. Upon termination of the TOU and/or DPA, Maile
upon the Customer's written request that deletes Customer Data in its

Stop War! Help Ukraine!
See what you can do

possession or control. This requirement shall not apply to the extent MailerLite is required by the applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data MailerLite shall securely isolate and protect from any further processing, except to the extent required by applicable law.

10. Customer Data Breach Management

10.1. MailerLite will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach with respect to Customer Data transmitted, stored or otherwise Processed by MailerLite or its Sub-Processors (a "*Customer Data Breach*"). Such notice may be provided (1) by posting a notice in the Services; (2) by sending an email to the email address from which the account of Authorized User was created; and/or (3) pursuant to the notice provisions of the TOU. The Customer shall ensure that its contact information is current and accurate at all times during the terms of this DPA. MailerLite will promptly take all actions relating to its Security Measures (and those of its Sub-Processors) that it deems necessary and advisable to identify and remediate the cause of a Customer Data Breach. In addition, MailerLite will promptly provide the Customer with: (i) reasonable cooperation and assistance with regard to the Customer Data Breach, (ii) reasonable information in MailerLite's possession concerning the Customer Data Breach insofar as it affects the Customer, including remediation efforts and any notification to Supervisory Authorities and, (iii) to the extent known: (a) the possible cause of the Customer Data Breach; (b) the categories of Customer Data involved; and (c) the possible consequences to Data Subjects. MailerLites's notification of or response to a Customer Data Breach under this Section will not constitute an acknowledgment of fault or liability with respect to the Customer Data Breach, and the obligations herein shall not apply to Personal Data Breaches that are caused by the Customer, Authorized Users or providers of Customer components (such as systems, platforms, services, software, devices, etc.). If the Customer decides to notify a Supervisory Authority, Data Subjects or the public of a Customer Data Breach, the Customer will provide MailerLite with advance copies of the proposed notices and, subject to applicable law (including any mandated deadlines under EU Data Protection Law), allow MailerLite an opportunity to provide any clarifications or corrections to those n
applicable law, MailerLite will not reference the Cu

Stop War! Help Ukraine!
See what you can do

notices or press releases associated with the Customer Data Breach without the Customer's prior consent.

11. Compliance and Reviews

11.1. Upon request, MailerLite shall supply, on a confidential basis, a copy of its audit reports (if any) to the Customer, so that the Customer can verify MailerLite's compliance with the audit standards and this DPA.

11.2. MailerLite shall also provide written responses, on a confidential basis, to all the Customer's reasonable requests for information to confirm MailerLite's compliance with this DPA.

11.3. Where required by EU Data Protection Law, MailerLite will allow the Customer (directly or through a third-party auditor subject to written confidentiality obligations) to conduct an audit of MailerLite's procedures relevant to the protection of Customer Data to verify MailerLite's compliance with its obligations under this DPA. In such case:

(a) The Customer shall: (i) provide MailerLite at least 30 days' prior written notice of any proposed audit; (ii) undertake an audit no more than once in any 12-month period, except where required by a competent Supervisory Authority or where an audit is required due to a Customer Data Breach; and (iii) conduct any audit in a manner designed to minimize disruption of MailerLite's normal business operations. To that end and before the commencement of any such audit, the Customer and MailerLite shall mutually agree upon any reimbursement of expenses for which the Customer shall be responsible as well as audit's participants, schedule and scope, which shall in no event permit the Customer or its third-party auditor to access the Services' hosting sites, underlying systems or infrastructure.

(b) Representatives of the Customer performing an audit shall protect the confidentiality of all information obtained through such audits in accordance with the TOU, may be required to execute an enhanced mutually agreeable nondisclosure agreement and shall abide by MailerLite's security policies while on MailerLite's premises. Upon completion of an audit, the Customer agrees to promptly furnish to MailerLite any written audit report or, if no written report is prepared, to promptly notify Maile
compliance discovered during the course of the au

Stop War! Help Ukraine!
See what you can do

12. Impact Assessment and Additional Information

12.1. MailerLite shall provide the Customer with reasonable cooperation and assistance needed to fulfill the Customer's obligation under EU Data Protection Law, to the best of abilities and as far as our resources allow, including:

(a) Carrying out a data protection impact assessment related to the Customer's use of the Services, to the extent the Customer does not otherwise have access to the relevant information, and to the extent such information is available to MailerLite.

(b) Providing reasonable assistance to the Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section to the extent required by EU Data Protection Law.

13. International Transfers

13.1. The Customer acknowledges that MailerLite may transfer and process Customer Data anywhere in the world where MailerLite, its affiliates or its Sub-Processors maintain data processing operations. MailerLite shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

13.2. To the extent that MailerLite is a recipient of Customer Data protected by EU Data Protection Laws ("EU Data") in a country outside of Europe that is not recognized as providing an adequate level of protection for personal data (as described in applicable EU Data Protection Law), the parties agree that MailerLite shall abide by and process EU Data in compliance with the SCCs in the form set out in **Annex 3**. For the purposes of the descriptions in the SCCs, MailerLite agrees that it is the "data importer" and the Customer is the "data exporter" (notwithstanding that the Customer may itself be an entity located outside Europe).

13.3. Sub-Processors used by MailerLite to Process any Customer Data protected by Data Protection Laws and/or that originates from the EEA, in a country that has not been designated by the Europ
Federal Data Protection Authority (as applicable) v

Stop War! Help Ukraine!
See what you can do

level of protection for Personal Data and have SCCs integrated in their Data Processing Agreements.

13.4. UK Data Transfers: the SCCs apply to transfers that fall under the UK Data Protection Laws, and they will be modified according to the specifications mentioned in the UK Addendum. The UK Addendum is considered as agreed upon by the parties and is included as an essential part of this DPA. The required information to complete Tables 1 to 3 in Part 1 of the UK Addendum will be obtained from the details provided in Annexes I and II of the relevant SCCs, and "neither party" will be selected to complete Table 4 in Part 1 of the UK Addendum.

14. Processing as Controller

14.1. The Parties believe MailerLite's role is as a Processor with respect to Customer Data. In relation to the Processing of Account Data, and to the extent (if any) that MailerLite may be considered a Controller in relation to certain Processing of Customer Personal Data, each Party will comply with its obligations as a Controller and agrees to provide reasonable assistance as is necessary: (a) to each other to enable each Party to comply with any Data Subject access requests and to respond to any other queries or complaints from Data Subjects in accordance with the EU Data Protection Law; and (b) to each other to facilitate the handling of any Personal Data Breach as required under EU Data Protection Law.

15. Limitation of Liability and Applicable Law

15.1. Each Party's liability taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the TOU.

16. Miscellaneous Provisions

16.1. Any claims brought under or in connection with this DPA are subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the TOU.

16.2. No one other than a Party to this DPA, its suc
assignees shall have any right to enforce any of its

Stop War! Help Ukraine!
See what you can do

16.3. Any claims against MailerLite under this DPA shall be brought solely against the entity that is a Party to the DPA. In no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. The Customer further agrees that any regulatory penalties incurred by MailerLite in relation to the Customer Data that arise as a result of, or in connection with, the Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce MailerLite's liability under the DPA.

16.4. This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the TOU, unless required otherwise by applicable Data Protection Laws.

16.5. The Customer ensures that the decision to agree with the terms and conditions of this DPA was made lawfully by the Customer, in case the Customer is a natural person, or, by the Customer's director, authorized representative or other person having signatory powers, in case the Customer is a legal person.

16.6. This DPA replaces any previous DPAs concluded between MailerLite and the Customer.

16.7. This DPA enters into force:

16.7.1. from the day you agreed with our Terms of Use and continues for an indefinite period of time; or

16.7.2. on July 1, 2021 if you have become our client before June 17, 2021 and continues for an indefinite period of time.

Annex 1

Details of Data Processing

1. Subject matter: The subject matter of the data Processing under this DPA is the Customer Data.

2. Duration of Processing: MailerLite will Process Customer Data for the duration of the Services, as described in the TOU.

Stop War! Help Ukraine!
See what you can do

3. Nature of the Processing: MailerLite provides email marketing and automation software as a service and other related services, as described in the TOU.

4. Purpose of the Processing: The purpose of the data Processing under this DPA is the provision of the Services.

5. Categories of Data subjects:

5.1. "Users" - any individual accessing and/or using the Services through the Customer's account;

5.2. "Subscribers" - any individual whose email address is included in the Customer's distribution list / whose information is stored on or collected via the Services / to whom Users send emails or otherwise engage or communicate with via the Services.

6. Types of Customer Data:

6.1. Users: identification and contact data (name, contact details, including email address, username); billing information (billing address, payment information); organization information (name, address, geographic location, area of responsibility, VAT code), IT information (IP address, usage data, cookies data, online navigation data, location data, browser data, access device information);

6.2. Subscribers: email address and any other additional information that Customer provides to MailerLite.

7. The Customer acknowledges that MailerLite shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as account management, technical support, product development or other. To the extent any such data is considered Personal Data under Data Protection Laws, MailerLite is the Data Controller of such data and accordingly shall process such data in accordance with MailerLite's Privacy Policy and Data Protection Laws.

8. The Customer acknowledges that in connection with the performance of the Services, MailerLite employs the use of cookies, unique identifiers, web beacons and similar tracking technologies. The Cu
appropriate notice, consent, opt-in and opt-out me

Stop War! Help Ukraine!
See what you can do

by Data Protection Laws to enable MailerLite to deploy previously mentioned tracking technologies lawfully on and collect data from the devices of Subscribers. The Customer may use this statement about MailerLite in the Customer's Privacy Policy:

"We use MailerLite to manage our email marketing subscriber list and to send emails to our subscribers. MailerLite is a third-party provider, which may collect and process your data using industry standard technologies to help us monitor and improve our newsletter. MailerLite's Privacy Policy is available at https://www.mailerlite.com/privacy-policy..

You can unsubscribe from our newsletter by clicking on the unsubscribe link provided at the end of each newsletter.".

Annex 2

Security Measures

Certain of MailerLite's Security Measures as of the date of this DPA:

1. Data Minimisation, Access Control and Employees Education

1.1. MailerLite collects and processes only that personal data that is necessary for the provision of services. However, clients decide themselves what personal data should be transferred to MailerLite for transactional email purposes.

1.2. MailerLite restricts access to Customer Data to employees with a defined need-to-know or a role requiring such access.

1.3. MailerLite's employees are introduced with the best security practices which allow them to identify Customer Data Breach and take any actions needed.

2. Business Continuity

2.1. MailerLite maintains business continuity and backup plans in order to minimize the loss of service and comply with applicable laws.

2.2. The Backup plan addresses threats to the Ser
dependencies, and has an established procedure f

Stop War! Help Ukraine!
See what you can do

use of, the Services.

2.3. The Backup plan is tested at regular intervals.

2.4. Management meetings regarding the determination of the information security risks arising to MailerLite are held annually. Management committee determines the risks, discusses them and searches for ways to prevent them.

3. Change Control

3.1. MailerLite maintains policies and procedures for applying changes to the Services, including underlying infrastructure and system components, to ensure quality standards are being met.

3.2. MailerLite undergoes a penetration test of its network and Services on an annual basis. Any vulnerabilities found during this testing will be remediated in accordance with MailerLite's procedures.

4. Data Security

4.1. MailerLite maintains technical safeguards and other security measures to ensure the security and confidentiality of Customer Data.

4.2. MailerLite's system is multi-tenant, therefore data is separated for users/accounts. Users don't have access to databases, so MailerLite manages it in its own way with sharding.

4.2. MailerLite uses Google data storage center with its location in the European Union. Google has information storage security certificate (ISO 27001) that ensures safety of Customer Data. Google data centers are protected with several layers of security to prevent any unauthorized access to your data. Google uses secure perimeter defense systems, comprehensive camera coverage, biometric authentication, and a 24/7 guard staff.

5. Encryption and Key Management

5.1. MailerLite maintains policies and procedures for the management of encryption mechanisms and cryptographic keys in MailerLite's cryptosystem. MailerLite ensures security over SSL/TLS and AES256 encryption.

5.2. MailerLite enlists encryption at rest and in tran
networks, as applicable, according to industry-sta

Stop War! Help Ukraine!
See what you can do

6. Data Transfer to Sub-Processors

6.1. Where sub-processors process the Personal Data of Subscribers, MailerLite takes steps to ensure that such sub-processors are service providers with whom MailerLite has entered into a contract that includes terms substantially similar to this DPA. MailerLite conducts appropriate due diligence on its sub-processors.

Annex 3

Standard Contractual Clauses (Transfer Controller to Processor)

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, [illegible] subject rights and effective legal remedies, pursuant to Article 46(1) and

Stop War! Help Ukraine!
See what you can do

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – 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 define
2016/679, those terms shall have the same meanir

Stop War! Help Ukraine!
See what you can do

(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

Stop War! Help Ukraine!
See what you can do

(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 t
personal data processed on behalf of the data exp

Stop War! Help Ukraine!
See what you can do

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).

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 com

Stop War! Help Ukraine!
See what you can do

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. 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, 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.

(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.

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 t
same country as the data importer or in another th

Stop War! Help Ukraine!
See what you can do

'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:(i) 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;(ii) 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;(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or(iv) 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

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

(b) 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.

(c) 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.

(d) 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.

(e) 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

Stop War! Help Ukraine!
See what you can do

(a) 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 10 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.

(b) 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.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 the data importer is subject pursuant to these Clauses.

(c) 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.

(d) 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.

(e) 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 dat
has received from a data subject. It shall not respo

Stop War! Help Ukraine!
See what you can do

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. 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.

Stop War! Help Ukraine!
See what you can do

(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.

(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

Stop War! Help Ukraine!
See what you can do

(a) 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.

(b) 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 d
requiring the disclosure of data to public authoritie

Stop War! Help Ukraine!
See what you can do

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.

Stop War! Help Ukraine!
See what you can do

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 promptly where it is unable to comply with these C

Stop War! Help Ukraine!
See what you can do

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 th

Stop War! Help Ukraine!
See what you can do

(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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Lithuar

Stop War! Help Ukraine!
See what you can do

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 Lithuania.(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.

APPENDIX to the Standard Contractual Clauses

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Customer, as those terms are defined in the MailerLite's Terms of Use to which the Data Processing Addendum is attached.

Data importer(s):

1. Name: MailerLite, Inc.

Address: 548 Market St, PMB 98174, San Francisco, California 94104-5401 US.

Contact person's name, position and contact details: info@mailerlite.com

Activities relevant to the data transferred under these Clauses: email marketing services

Signature and date: enters into force on 2021/09/24; in case Customer becomes our client on or later than 2021/09/24, it enters into force on the day when Customer agreed with our Terms of Use.

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Customer determines and controls the extent of Customer Personal Data submitted for Processing by the Services, which may include Pe
Users - any individual accessing and/or using the

Stop War! Help Ukraine!
See what you can do

Customer's account; (2) Subscribers - any individual whose email address is included in the Customer's distribution list / whose information is stored on or collected via the Services / to whom Users send emails or otherwise engage or communicate with via the Services.

Categories of personal data transferred: The personal data transferred concern the following categories of data: (1) Users: identification and contact data (name, contact details, including email address, username); billing information (billing address, payment information); organization information (name, address, geographic location, area of responsibility, VAT code), IT information (IP address, usage data, cookies data, online navigation data, location data, browser data, access device information); (2) Subscribers: email address and any other additional information that Customer provides to MailerLite.

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: No sensitive data shall be transferred to MailerLite.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Data is transferred on a continuous basis for the duration of the Services, as described in the TOU.

Nature of the processing: MailerLite is a service that provides clients with a means to collect email addresses and to create, send and track email promotions ("**Services**") and other services pursuant to any order confirmations, ordering documents or online registration, as described in the TOU.

Purpose(s) of the data transfer and further processing: The purpose of the data Processing under this DPA is the provision of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Data will be retained for the duration of Services. It shall not apply to the e
by the applicable law to retain some or all of the C

Stop War! Help Ukraine!
See what you can do

Customer Data it has archived on back-up systems where Customer Data is securely isolated and protected from any further processing, except to the extent required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Personal Data might be transferred to MailerLite's sub-processors in order to provide its clients with the Services. Sub-processing should take place for the duration of the provision of Services or longer, if required by law.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: State Data Protection Inspectorate of the Republic of Lithuania.

ANNEX II

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

Please see Annex 2 of DPA – Security Measures.

ANNEX III

LIST OF SUB-PROCESSORS

Please see Annex 4 of DPA – List of MailerLite Sub-Processors.

Annex 4

List of MailerLite Sub-Processors

MailerLite uses a range of third-party Sub-Processors to assist it in providing the Services (as described in the DPA).

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

1.Name: **Google Ireland Limited**

Stop War! Help Ukraine!
See what you can do

Address: Gordon House, Barrow Street, Dublin 4, Dublin, D04e5w5, Ireland

Contact person's name, position and contact details: you may contact using their website https://support.google.com/policies/contact/general_privacy_form

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Data center with its location in Germany

2.Name: **Vercom S.A.**

Address: Roosevelta 22, 60-829 Poznań, Poland

Contact person's name, position and contact details: Data Protection Officer, Mrs. Marika Rybarczyk, at: iod@vercom.pl

Description of processing: Managing and improving MailerLite services as a shareholder

Last updated on May 4, 2023

PRODUCT

Email marketing

Automations

Websites

Integrations

Compare MailerLite

Compare to Substack

Compare to Ghost

SUPPORT

Knowledge base

Video tutorials

Academy

Hire an Expert

Migration service

Support

Report abus

Stop War! Help Ukraine!

See what you can do

Developer API

What's new

COMPANY

About us

Why Lite

Company values

Jobs

Become a partner

Contact us

Wall of love

Let's keep in touch

Sign up for our weekly email marketing newsletter and MailerLite updates.

Enter your email

Subscribe

For more details, review our Privacy Policy.

2010 - 2023 © MailerLite. All rights reserved.

Terms of Service Cookies Settings Brand Assets

GDPR Compliant
Your data is safe with us

Download on the App Store

Stop War! Help Ukraine!
See what you can do

Stop War! Help Ukraine!
See what you can do