MailChimp Additional Terms for Data Processing

1 messaggio

MailChimp Legal Team <legal@mailchimp.com> 12 marzo 2016 17:27
A: Alessandra Farabegoli <info@digitalupdate.it>

MailChimp Additional Terms for Data Processing - In Compliance with the Standard Contractual Clauses

These Additional Terms for Data Processing (the “Processing Terms”) are entered into as of the 12 day of March, 2016, by and between The Rocket Science Group, LLC, a limited liability company organized in the State of Georgia, ("we," "us," "our" “MailChimp” or “data importer”) and Alessandra Farabegoli, ("you," “data exporter” “your” or “User") a resident of or an entity located in Italy (collectively the “Parties” and individually a “Party.”)

We offer the services MailChimp, TinyLetter, and Mandrill (collectively the “Service”) through the URL www.mailchimp.com, www.tinyletter.com, and www.mandrill.com (the “Websites”) which allow you to create, send, and manage email newsletters to recipients. You have signed up for the Service and have agreed to our Terms of Use (including our Privacy Policy, Acceptable Use Policy, API Guidelines, and Brand Guidelines, collectively the “Terms” or the “Agreement”). For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection the parties 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.

Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘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 (1);

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of 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 controller in the Member State in which the data exporter is established;

(f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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 subprocessor 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 organisational 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, unauthorised 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 subprocessor 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

Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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 organisational 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 prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- **(ii)** any accidental or unauthorised access; and
- **(iii)** any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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, namely Italy

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 fulfil 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, namely Italy

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, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or 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.

Signed:

The Rocket Science Group, LLC

By: Daniel Kurzius, CCO/Co-founder

Alessandra Farabegoli

By: Alessandra Farabegoli, founder

Appendix 1

Data exporter

The data exporter is an individual or entity that has contracted with MailChimp or one of MailChimp's products (TinyLetter or Mandrill) for email marketing services. Activities relevant to the transfer include: newsletters, promotions, market research, advertisements, offers, general updates, and communications regarding services offered by the data exporter.

Data importer

The data importer is an email service provider that allows users to store, create, send, target, and track email addresses and email campaigns.

Data subjects

The personal data transferred may concern the following categories of data subjects: customers, clients, prospective customers and clients, students, donors, and employees.

Categories of data

The personal data transferred may concern the following categories of data: name, gender, birthdate, language, email address, telephone number, home address, employer, work address, title, expertise, other demographic information, purchase history, and event attendance. Data will not include Social Security numbers or other national ID numbers, passwords, security credentials, or sensitive personal information of any kind.

Processing operations

The personal data transferred will be subject to the following basic processing activities: storage; access for customer service; in accordance with your use of features; abuse detection, prevention, and remediation; maintaining, improving, and providing our Services.

Data exporter expressly authorizes data importer to respond to the following requests received directly from the data subjects: unsubscribes, updates to information, removal of information, or a block of that data subject's information from being stored in data importer's system.

Subprocessors

Data exporter consents to subprocessing by the following subcontractors: Amazon, Akamai, DissectCyber, E-Hawk, El Camino, Evernote, Google, HipChat, Liveperson, MailMonitor, Softlayer.

Signed:

The Rocket Science Group, LLC

By: Daniel Kurzius, CCO/Co-founder

Alessandra Farabegoli

By: Alessandra Farabegoli, founder

Appendix 2

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):

Data Center Security

- Data importer delivers more than 20 billion emails a month for more than 10 million users. We use multiple MTAs, placed in different world-class data centers, around the US.
- Our data centers manage physical security 24/7 with biometric scanners, and the usual high tech stuff that data centers always brag about.
- We have DDOS mitigation in place at all our data centers.
- We have a documented "in case of nuclear attack on a data center" infrastructure continuity plan.

Protection from Data Loss, Corruption

- All large account databases are kept separate and dedicated to prevent corruption and overlap. Smaller and free user accounts are placed into the same large database for speed. As accounts grow in list size, they are migrated into their own distinct databases.
- Account data is mirrored and backed up regularly off site.

Application Level Security

- User account passwords are hashed. Our own staff can't even view them. If you lose your password, it can't be retrieved—it must be reset.
- All login pages (from our website and mobile website) pass data via SSL.
- The entire application is encrypted with SSL.
- Login pages have brute force protection.
- Logins via the MailChimp API have brute force protection.
- We perform regular security penetration tests, using different vendors. The tests involve high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.

Mobile App Security

- Sensitive data on iPhone apps are stored in Keychain for security.
- Sensitive data is transmitted via SSL.
- TRUSTe verifies compliance on relevant apps.

Internal IT Security

- Our office is secured by keycard access, and is monitored with infrared cameras throughout.

Internal Protocol & Education

- All new employees on teams that have access to customer data (such as tech support and our engineers) undergo criminal history and credit background checks prior to employment.
- The Art of Deception, by Kevin Mitnick, is required reading for all new employees. Fatal System Error, by Joseph Menn, is extra credit.
- All employees sign a Privacy Safeguard Agreement outlining their responsibility in protecting customer data.
- All new employees are given security guidelines for using social media, including information about social engineering.
- We have an employee termination (AKA: "change management") process in place.
- In order to protect our company from a variety of different losses, we have established a comprehensive insurance program. This program has been designed to cover us for standard business losses that all businesses can face as well as those losses that are unique to what we do in the technology industry. Additionally, we have selected a carrier that is financially strong and purchased substantial limits for the following general coverages:
    - Property and Business Interruption
    - Commercial General Liability
    - Workers Compensation and Employers Liability
    - Business Automobile
    - Umbrella Liability
    - International Property and Liability
    - Technology Errors & Omissions Liability
    - Management Liability

We're SOC II Compliant and have PCI DSS Certification. We're happy to provide our full SOC II Report upon request.

Signed:

The Rocket Science Group, LLC

By: Daniel Kurzius, CCO/Co-founder

Alessandra Farabegoli

By: Alessandra Farabegoli, founder
