Betreff: MailChimp Data Processing Addendum
Von: MailChimp Legal Team <dpa@mailchimp.com>
Datum: 18.05.18, 10:56
An: Urs Zulauf <office@casfinreg.ch>

Customer EU Data Processing Addendum

This Data Processing Addendum ("**DPA**"), forms part of the Agreement between The Rocket Science Group LLC d/b/a MailChimp ("**MailChimp**") and CAS Financial Regulation ("**Customer**") and shall be effective on the date both parties execute this DPA (**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"**Agreement**" means MailChimp's Terms of Use, which govern the provision of the Services to Customer, as such terms may be updated by MailChimp from time to time.

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" shall be construed accordingly.

"**Customer Data**" means any Personal Data that MailChimp processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

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

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

"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"**Group**" means any and all Affiliates that are part of an entity's corporate group.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

"**Services**" means any product or service provided by MailChimp to Customer pursuant to the Agreement.

"**Sub-processor**" means any Data Processor engaged by MailChimp or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or members of the MailChimp Group.

2. Relationship with the Agreement

2.1 The parties agree that DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.

2.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

2.3 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

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

2.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

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

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that MailChimp processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

3.2 Part A (being Section 4 – 8 (inclusive) of this DPA, as well as Annexes A and B of this DPA) shall apply to the processing of Customer Data within the scope of this DPA from the Effective Date.

3.3 Part B (being Sections 9-12 (inclusive) of this DPA) shall apply to the processing of Customer Data within the scope of the DPA from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

Part A: General Data Protection Obligations

4. Roles and Scope of Processing

4.1 **Role of the Parties**. As between MailChimp and Customer, Customer is the Data Controller of Customer Data, and MailChimp shall process Customer Data only as a Data Processor acting on behalf of Customer.

4.2. **Customer Processing of Customer Data**. Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to MailChimp; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for MailChimp to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

4.3 **MailChimp Processing of Customer Data**. MailChimp shall process Customer Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to MailChimp in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and MailChimp.

4.4 **Details of Data Processing**

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration: As between MailChimp and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of MailChimp's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(d) Nature of the processing: MailChimp provides an email service, automation and marketing platform and other related services, as described in the Agreement.

(e) Categories of data subjects: Any individual accessing and/or using the Services through the Customer's account ("**Users**"); and any individual: (i) whose email address is included in the Customer's Distribution List; (ii) whose information is stored on or collected via the Services, or (iii) to whom Users send emails or otherwise engage or communicate with via the Services (collectively, "**Subscribers**").

(f) Types of Customer Data:

(i) Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);

(ii) Subscribers: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publically available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

4.5 Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that MailChimp 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 billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, MailChimp is the Data Controller of such data and accordingly shall process such data in accordance with the MailChimp Privacy Policy and Data Protection Laws.

4.6 **Tracking Technologies**. Customer acknowledges that in connection with the performance of the Services, MailChimp employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("**Tracking Technologies**"). Customer shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable MailChimp to deploy Tracking Technologies lawfully on, and collect data from, the devices of Subscribers (defined below) in accordance with and as described in the MailChimp Cookie Statement.

5. Subprocessing

5.1 **Authorized Sub-processors**. Customer agrees that MailChimp may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by MailChimp and authorized by Customer are listed in **Annex A**.

5.2 **Sub-processor Obligations**. MailChimp shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause MailChimp to breach any of its obligations under this DPA.

6. Security

6.1 **Security Measures**. MailChimp shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with MailChimp's security standards described in **Annex B** ("**Security Measures**").

6.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by MailChimp relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that MailChimp may update or modify the Security Measures 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.

6.3 **Customer Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication 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. Security Reports and Audits

7.1 Customer acknowledges that MailChimp is regularly audited against SSAE 16 and PCI standards by independent third party auditors and internal auditors, respectively. Upon request, MailChimp shall supply (on a confidential basis) a summary copy of its audit report(s) ("**Report**") to Customer, so that Customer can verify MailChimp's compliance with the audit standards against which it has been assessed, and this DPA.

7.2 MailChimp shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm MailChimp's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

8. International Transfers

8.1 **Data center locations**. MailChimp may transfer and process Customer Data anywhere in the world where MailChimp, its Affiliates or its Sub-processors maintain data processing operations. MailChimp shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

8.2 **Privacy Shield**. To the extent that MailChimp processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that MailChimp shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by virtue of having self-certified its compliance with Privacy Shield. MailChimp agrees to protect such Personal Data in accordance with the requirements of the Privacy Shield Principles. If MailChimp is unable to comply with this requirement, MailChimp shall inform Customer.

8.3 **Alternative Transfer Mechanism**. The parties agree that the data export solution identified in Section 8.2 shall not apply if and to the extent that MailChimp adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under EU Data Protection Laws) outside of the EEA ("**Alternative Transfer Mechanism**"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

Part B: GDPR Obligations from 25 May 2018

9. Additional Security

9.1 **Confidentiality of processing**. MailChimp shall ensure that any person who is authorized by MailChimp to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2 **Security Incident Response**. Upon becoming aware of a Security Incident, MailChimp shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

10. Changes to Sub-processors

10.1 MailChimp shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email shall suffice) if it adds or removes Sub-processors at least 10 days prior to any such changes.

10.2 Customer may object in writing to MailChimp's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Agreement, MailChimp shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent MailChimp is required by 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 MailChimp shall securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Cooperation

12.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, MailChimp shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to MailChimp, MailChimp shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If MailChimp is required to respond to such a request, MailChimp shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

12.2 If a law enforcement agency sends MailChimp a demand for Customer Data (for example, through a subpoena or court order), MailChimp shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, MailChimp may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then MailChimp shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless MailChimp is legally prohibited from doing so.

12.3 To the extent MailChimp is required under EU Data Protection Law, MailChimp shall (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

The Rocket Science Group LLC d/b/a MailChimp

By:

Name: Daniel Kurzius
Title: CCO/Co-founder
Date: May 18, 2018

CAS Financial Regulation

Name: Urs Zulauf
Title: Study director
Date: May 18, 2018

Annex A - List of MailChimp Sub-processors

MailChimp uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services (as described in the Agreement). These Sub-processors set out below provide cloud hosting and storage services; content delivery and review services; assist in providing customer support; as well as incident tracking, response, diagnosis and resolution services.

Entity Name	Corporate Location
Akamai	Massachusetts, USA
Amazon	Washington, USA
E-Hawk	New York, USA
El Camino	California, USA
FullContact	Colorado, USA
Google	California, USA
Neustar	Virginia, USA
R.R. Donnelley	Illinois, USA
Slack	California, USA
TaskUs	California, USA
Zendesk	California, USA

Annex B – Security Measures

The Security Measures applicable to the Services are described here https://mailchimp.com/about/security/ (as updated from time to time in accordance with Section 6.2 of this DPA).