RECORD
of processing activity[1]
according to Article 31 Regulation 2018/1725[2]

NAME of data processing[3]:
Subscription to F4E Electronic Newsletter

Last update: March 2020

1) Controller(s)[4] of data processing operation (Article 31.1(a))

- Controller: Organisational entity of Fusion for Energy (F4E)
  - Unit / Department **responsible[5]** for the processing activity: *Communication Unit*
  - Contact: Communications@f4e.europa.eu
- Data Protection Officer (DPO): DataProtectionOfficer@f4e.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[6]

The data is processed by F4E (responsible unit) itself ..... ☒

The data is processed by a third party (e.g. contractor) (Art. 29 – Processor) : ..... ☒

Rocket Science Group (mailchimp)

[https://mailchimp.com/legal/privacy/]

Contact point at external third party (e.g. Privacy/Data Protection Officer):

1 Please consult the relevant **EDPS guideline** in your sector, if it exists: https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

2 Regulation 2018/1725 of 23 October 2018 "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data". O.J 21.11.2018, L295/39.

3 **Personal data** is *any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity*. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.
Processing means *any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*.

4 In case of more than one controller, see Article 28.

5 This is the unit that decides that the processing takes place and why.

6 Is F4E itself conducting the processing? Or has a provider been contracted?

3) Purpose and Description of the processing (Article 31.1(b))

Why is the personal data being processed? Specify the underlying reason for the processing and what you intend to achieve. Describe, summarise the substance of the processing.

When you (later on) intend to further process the data for another purpose, please inform the Data Subject in advance.

The purpose of processing these data is to:

- have the necessary information to deliver the F4E Electronic Newsletter and

- to identify very generic information of the readers to better focus on the content of our newsletter.

4) Lawfulness of the processing (Article 5(a)–(d)):

Mention the legal bases which justifies the processing

Processing necessary for:

(a) performance of tasks in the public interest attributed by EU legislation (including management and functioning of F4E) ..... ☒

- Council Decision of 27 March 2007 "establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it" - 2007/198/Euratom, as last amended by Council Decision of 22 February 2021 (2021/281 Euratom), O.J. L 62, 23.02.2021, p.8, in particular Article 6 thereof;

- Statutes annexed to the Council Decision (Euratom) No 198/2007 "establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it", as last amended on 22 February 2021, in particular Article 10 thereof;Staff Regulations of Officials (SR) and the Conditions of Employment of Other Servants of the European Communities (CEOS), in particular

(b) compliance with a *specific* legal obligation for F4E to process personal data[7]..... ☐

(c) necessary for the performance of a contract with the data subject or to prepare such a contract ..... ☐

(d) Data subject has given consent (ex ante, freely given, specific, informed and unambiguous consent) ..... ☒

[7] The distinction between points (a) and (b) is that in point (a) F4E is given a task which requires the processing of personal data to fulfil it (e.g. staff appraisal), while in point (b), the legal basis directly requires F4E to process the personal data, without margin of implementation.

Consent is given when subscribing to the newsletter. It is stored in a secure data base platform.

5) Description of the data subjects (Article 31.1(c))

Whose personal data is being processed?

Electronic newsletter's subscribers.

6) Categories of personal data processed (Article 31.1(c))

Please give details in relation to (a) and (b). In case data categories differ between different categories of data subjects, please explain as well.

(a) **General personal data:**
Identification Data:
E-mail addresses
Professional activity
Country (of origin//of residence) of the subscribers

(b) **Sensitive personal data** (Article 10)
No sensitive personal data are processed.

7) Recipient(s) of the data (Article 31.1 (d)) – Who has access to the personal data?

Recipients are all people to whom the personal data is disclosed ("need to know principle"). Not necessary to mention entities that may have access in the course of a particular investigation (e.g. OLAF,Court, EDPS).

The following recipients have access to the personal data processed:

- Communication Unit and The Rocket Science Group (mailchimp)
- IDM Manager, if necessary for support,
- ICT Officer responsible for the dedicated database, if necessary for technical support.

Also, only if appropriate and necessary for monitoring or inspection tasks, access may be given to: e.g. F4E Director Head of Admin., DPO and Anti-Fraud & Ethics Officer, Head or responsible officer of LSU, IAC, IDOC.

8) Transfers to third countries or International Organizations (Article 31.1 (e))

If the personal data is transferred outside the EU, this needs to be specifically mentioned, since it increases the risks of the processing operation (Article 47 ff.).

Data is transferred to third countries or International Organizations recipients:

Yes ..... ☒

No ..... ☐

If yes, specify to which country/IO: Mailchimp may transfer and process Customer Data to and in the United States and anywhere else in the world where Mailchimp, its Affiliates or its Sub-processors maintain data processing operations

If yes, specify under which safeguards and add reference :

- Adequacy Decision (from the Commission) ..... ☐
- Memorandum of Understanding between public authorities/bodies ..... ☐
- Standard Data Protection Clauses (from the EDPS/Commission) ..... ☐
- Binding Corporate Rules ..... ☐
- Others, e.g. contractual/agreements (subject to authorisation by the EDPS) ..... ☒

Reference:

Mailchimp Data Processing Addendum
(https://mailchimp.com/legal/data-processing-addendum/)

9) Technical and organisational security measures (Articles 31.1(g) and 33)

Please specify where the data is stored (paperwise and/or electronically) during and after the processing. Specify how it is protected ensuring "confidentiality, integrity and availability". State in particular the "level of security ensured, appropriate to the risk".

Security measures are implemented to ensure integrity, confidentiality and availability of information. The default provisions include backups, centralized logging, software updates and continuous vulnerability assessment and follow-up. Specific provisions resulting from the characteristics of the information system may lead into the implementation of encryption, two factor authentication among others found relevant following a risk analysis

10) Retention time (Article 4(e))

How long is it necessary to retain the data and what is the justification for this retention period? If appropriate, differentiate between the categories of personal data. If the retention period is unknown, please indicate the criteria for determining it.

Data will be kept as long as the subscription is active.

11) Information/Transparency (Article 14-15) *Information shall be given in a concise, transparent and easily accessible form, using clear and plain language.*
PN to be published on the website (subscription part)

LEGAL

Privacy Policy

In this document

Effective January 1, 2020
View the prior version of our privacy policy (last updated December 5, 2018) **here**.

Mailchimp takes data privacy seriously. This privacy policy explains who we are, how we collect, share and use Personal Information, and how you can exercise your privacy rights.

We recommend that you read this privacy policy in full to ensure you are fully informed. However, to make it easier for you to review the parts of this privacy policy that apply to you, we have divided up the document into sections that are specifically applicable to **Members** (Section 2), **Contacts** (Section 3), and **Visitors** (Section 4). Sections 1 and 5 are applicable to everyone.

If you have any questions or concerns about our use of your Personal Information, then please contact us using the contact details provided at the end of Section 5.

To the extent we provide you with notice of different or additional privacy policies, those policies will govern such interactions.

TRUSTe Verified Privacy Powered by TrustArc

1. The Basics

A. About Us

Mailchimp is an online marketing platform operated by The Rocket Science Group LLC, a company headquartered in the State of Georgia in the United States ("**we**," "**us**," "**our**," and "**Mailchimp**").

Our Service enables our Members to, among other things, send and manage email campaigns across channels, serve advertisements, and create Websites and Landing Pages. We also provide other related services, such as real-time data analytics and insights to help our Members track and personalize their marketing activities. Find out more about our Service **here**.

B. Key Terms

In this privacy policy, these terms have the following meanings:

"Mobile App(s)" means any one or all of the Mailchimp applications available for Members to use on their mobile devices.

"**Contact**" is a person a Member may contact through our Service. In other words, a Contact is anyone on a Member's Distribution List or about whom a Member has given us information. For example, if you are a Member, a subscriber to your email marketing campaigns would be considered a Contact.

"**Distribution List**" is a list of Contacts a Member may upload or manage on our platform and all associated information related to those Contacts (for example, email addresses).

"**Member**" means any person or entity that is registered with us to use the Service.

"**Personal Information**" means any information that identifies or can be used to identify an individual directly or indirectly. Examples of Personal Information include, but are not limited to, first and last name, date of birth, email address, gender, occupation, or other demographic information.

"Service" has the meaning given to it in our **Standard Terms of Use**.

"Mailchimp Site(s)" has the meaning given to it in our **Standard Terms of Use**.

"**Visitor**" means, depending on the context, any person who visits any of our Mailchimp Sites, offices, or otherwise engages with us at our events or in connection with our marketing or recruitment activities.

"**you**" and "**your**" means, depending on the context, either a Member, a Contact, or a Visitor.

2. Privacy for Members

This section applies to the Personal Information we collect and process from a Member or potential Member through the provision of the Service. If you are not a Member, the **Visitors** or **Contacts** section of this policy may be more applicable to you and your data. **In this section, "you" and "your" refer to Members and potential Members.**

A. Information We Collect

The Personal Information that we collect depends on the context of your interactions with Mailchimp, your Mailchimp account settings, the products and features you use, your location, and applicable law. However, the Personal Information we collect broadly falls into the following categories:

(i) **Information you provide to us**: You (or your organization) may provide certain Personal Information to us when you sign up for a Mailchimp account and use the Service, consult with our customer service team, send us an email, integrate the Service with another website or service (for example, when you choose to connect your e-commerce account with Mailchimp), or communicate with us in any other way.

This information may include:

- Business contact information (such as your name, job title, organization, location, phone number, email address, and country);
- Marketing information (such as your contact preferences);
- Account log-in credentials (such as your email address or username and password when you sign up for an account with us);
- Troubleshooting and support data (which is data you provide or we otherwise collect in connection with support queries we receive from you. This may include contact or authentication data, the content of your chats and other communications with us, and the product or service you are using related to your help inquiry); and

- Payment information (including your credit card numbers and associated identifiers and billing address).

(ii) **Information we collect automatically**: When you use the Service, we may automatically collect or receive certain information about your device and usage of the Service (collectively "Service Usage Data"). In some (but not all) countries, including countries in the European Economic Area ("EEA"), this information is considered Personal Information under applicable data protection laws. We use cookies and other tracking technologies to collect some of this information. If you are using our Mobile App, we may collect this information using our software development kits ("SDKs") or APIs the first time the SDK or API is initiated on your Mobile App. For further information, please review the section below and our Cookie Statement available **here**.

Service Usage Data may include:

- **Device information:** We collect information about the device and applications you use to access the Service, such as your IP address, your operating system, your browser ID, and other information about your system and connection. If you are using our Mobile App, we may also collect information about the cellular network associated with your mobile device, your mobile device's operating system or platform, the type of mobile device you use, your mobile device's name and unique device ID, and information about the features of our Mobile App that you accessed.
- **Log data:** Our web servers keep log files that record data each time a device accesses those servers and the nature of each access, including originating IP addresses and your activity in the Service (such as the date/time stamps associated with your usage, pages and files viewed, searches and other actions you take (for example, which features you used)), device event information (such as system activity, error reports (sometimes called 'crash dumps')), and hardware settings. We may also access metadata and other information associated with files that you upload into our Service.
- **Usage data:** We collect usage data about you whenever you interact with our Service, which may include the dates and times you access the Service and your browsing activities (such as what portions of the Service you used). We also collect information regarding the performance of the Service, including metrics related to the deliverability of emails and other communications you send through the Service. If you are using our Mobile App, we may collect information about how often you use the Mobile App and other performance data. This information allows us to improve the content and operation of the Service, and facilitate research and analysis of the Service.

(iii) **Information we collect from other sources:** From time to time, we may obtain information about you from third-party sources, such as public databases, social media platforms, third-party data providers, and our joint marketing partners.

Examples of the information we receive from other sources include demographic information (such as age and gender), device information (such as IP addresses), location (such as city and state), and online behavioral data (such as information about your use of social media websites, page view information and search results and links). We use this information, alone or in combination with other Personal Information we collect, to enhance our ability to provide relevant marketing and content to you and to develop and provide you with more relevant products, features, and service.

B. Use of Personal Information

We may use the Personal Information we collect or receive through the Service (alone or in combination with other data we source) for the purposes and on the legal bases identified below:

- To bill and collect money owed to us by you to perform our contract with you for the use of the Service or where we have not entered into a contract with you, in accordance with our legitimate interests to operate and administer our Service. This includes sending you emails, invoices, receipts, notices of delinquency, and alerting you if we need a different credit card number. We use third parties for secure credit card transaction processing, and those third parties collect billing information to process your orders and credit card payments. To learn more about the steps we take to safeguard that data, see the "Our Security" section of this privacy policy.
- To send you system alert messages in reliance on our legitimate interests in administering the Service and providing certain features. For example, we may inform you about temporary or permanent changes to our Service, such as planned outages, or send you account, security or compliance notifications, such as new features, version updates, releases, abuse warnings, and changes to this privacy policy.
- To communicate with you about your account and provide customer support to perform our contract with you for the use of the Service or where we have not entered into a contract with you, in reliance on our legitimate interests in administering and supporting our Service. For example, if you use our Mobile Apps, we may ask you if you want to receive push notifications about activity in your account. If you have opted in to these push notifications and no longer want to receive them, you may turn them off through your operating system.
- To enforce compliance with our Standard Terms of Use and applicable law, and to protect the rights and safety of our Members in reliance on our legitimate interest to protect against misuse or abuse of our Service and to pursue remedies available. This may include developing tools and algorithms that help

us prevent violations. For example, sometimes we review the content our Members send or display to ensure it complies with our Standard Terms of Use. To improve that process, we have software that helps us find content that may violate our Standard Terms of Use. We may or our third-party service provider may also review content that our Members send or display. This benefits all Members who comply with our Standard Terms of Use because it reduces abuse and helps us maintain a reliable platform. Please do not use Mailchimp to send or display confidential information.

- To meet legal requirements, including complying with court orders, valid discovery requests, valid subpoenas, and other appropriate legal mechanisms.
- To provide information to representatives and advisors, including attorneys and accountants, to help us comply with legal, accounting, or security requirements in reliance on our legitimate interests.
- To prosecute and defend a court, arbitration, or similar legal proceeding.
- To respond to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- To provide, support and improve the Service to perform our contract with you for the use of the Service or where we have not entered into a contract with you, in reliance on our legitimate interests in administering and improving the Service and providing certain features. For example, this may include sharing your information with third parties in order to provide and support our Service or to make certain features of the Service available to you. When we share your Personal Information with third parties, we take steps to protect your information in a manner that is consistent with our obligations under applicable privacy laws. For further information about how we share your information, refer to Section 5 below.
- To provide suggestions to you and to provide tailored features within our Service that optimize and personalize your experience in reliance on our legitimate interests in administering the Service and providing certain features. This includes adding features that compare Members' email campaigns, using data to suggest other publishers your Contacts may be interested in, or using data to recommend products or services that you may be interested in or that may be relevant to you or your Contacts. Some of these suggestions are generated through analysis of the data used in our data analytics projects, as described below.
- To perform data analytics projects in reliance on our legitimate business interests in improving and enhancing our products and services for our Members. Our data analytics projects use data from Mailchimp accounts, including Personal Information of Contacts, to provide and improve the Service. We use information like your sending habits and your Contacts' purchase history, so we can make more informed predictions, decisions, and products for our Members. For example, we use data from Mailchimp accounts to enable product recommendation, audience segmentation, and predicted demographics features for our Members. If you or your Contact prefers not to have their data used for this purpose, you can alter the settings on your account (as described **here**) to opt out of data analytics projects, or your Contact can

opt out of data analytics projects at any time by emailing us at personaldatarequests@mailchimp.com. As always, we take the privacy of Personal Information seriously, and will continue to implement appropriate safeguards to protect this Personal Information from misuse or unauthorized disclosure.

- To personalize the Service, content and advertisements we serve to you in reliance on our legitimate interests in supporting our marketing activities and providing certain features within the Service. We may use your Personal Information to serve you specifically, such as to deliver a product or service according to your preferences or restrictions, to provide more personalized features or for advertising or targeting purposes in accordance with this privacy policy.

C. Third-Party Integrations

We may use the Personal Information we collect or receive through the Service, as a processor and as otherwise stated in this privacy policy, to enable your use of the integrations and plugins you choose to connect to your Mailchimp account. For instance, if you choose to connect a Google integration to your Mailchimp account, we'll ask you to grant us permission to view and/or download, as applicable, your Google Sheets, Google Contacts, Google Analytics and Google Drive. This allows us to configure your Google integration(s) in accordance with your preferences. For example, if you wanted to use the Google Contacts integration to share the templates in your Mailchimp account with contacts in your Google address book, we would need to access your Google Contacts to share your templates.

D. Cookies and Tracking Technologies

We and our third-party partners may use various technologies to collect and store Service Usage Data when you use our Service (as discussed above), and this may include using cookies and similar tracking technologies, such as pixels, web beacons, and if you use our Mobile Apps, through our SDKs deployed on your mobile device. For example, we use web beacons in the emails we send on your behalf, which enable us to track certain behavior, such as whether the email sent through the Service was delivered and opened and whether links within the email were clicked. Both web beacons and SDKs allow us to collect information such as the recipient's IP address, browser, email client type and other similar data as further described above details. We use this information to measure the performance of your email campaigns, to provide analytics information, enhance the effectiveness of our Service, and for other purposes described above. Reports are also available to us when we send email to you, so we may collect and review that information.

Our use of cookies and other tracking technologies is discussed in more detail in our Cookie Statement available **here**.

E. Member Distribution Lists

In order to send an email campaign or use certain features in your account, you need to upload a Distribution List that provides us information about your Contacts, such as their names and email addresses. We use and process this information to provide the Service in accordance with our contract with you or your organization and this privacy policy.

A Distribution List can be created in a number of ways, including by importing Contacts, such as through a CSV or directly from your email client. We do not, under any circumstances, sell your Distribution Lists. If someone on your Distribution List complains or contacts us, we might then contact that person. You may export (download) your Distribution Lists from Mailchimp by accessing the "Audience" tab from within your account.

If we detect abusive or illegal behavior related to your Distribution List, we may share your Distribution List or portions of it with affected ISPs or anti-spam organizations to the extent permitted or required by applicable law.

If a Contact chooses to use the Forward to a Friend (FTF) link in an email campaign a Member sends, it will allow the Contact to share the Member's email content with individuals not on the Member's Distribution List. When a Contact forwards an email to a friend, we do not store the Contact's email address or their friend's email address, and no one is added to any Distribution List as a result of the FTF link. The Member who created the email campaign only sees an aggregate number of times their email campaign was forwarded by a Contact and does not have access to the email addresses used to share or receive that forwarded content.

F. Your Data Protection Rights

Depending on the country in which you reside, you may have the following data protection rights:

- To access; correct; update; port; delete; restrict; or object to our processing of your Personal Information.
- You can manage your individual account and profile settings within the dashboard provided through the Mailchimp platform, or you may contact us

directly by emailing us at personaldatarequests@mailchimp.com. You can also manage information about your Contacts within the dashboard provided through the Mailchimp platform to assist you with responding to requests to access, correct, update, port or delete information that you receive from your Contacts. Note, if any of your Contacts wish to exercise any of these rights, they should contact you directly, or contact us as described in the "Privacy for Contacts" section below. You can also contact us at any time to update your own marketing preferences (see Section 5. General Information, C. Your Choices and Opt-Outs below). Mailchimp takes reasonable steps to ensure that the data we collect is reliable for its intended use, accurate, complete and up to date.

- The right to complain to a data protection authority about the collection and use of Personal Information. For more information, please contact your local data protection authority. Contact details for data protection authorities in the EEA and UK are available **here** and Switzerland are available **here**.
- Similarly, if Personal Information is collected or processed on the basis of consent, the data subject can withdraw their consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect the processing of your Personal Information conducted in reliance on lawful processing grounds other than consent. If you receive these requests from Contacts, you can segment your lists within the Mailchimp platform to ensure that you only market to Contacts who have not opted out of receiving such marketing.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection law. We may ask you to verify your identity in order to help us respond efficiently to your request. If we receive a request from one of your Contacts, we will either direct the Contact to reach out to you, or, if appropriate, we may respond directly to their request.

3. Privacy for Contacts

This section applies to the information we process about our Members' Contacts as a data controller. Our Service is intended for use by our Members. As a result, for much of the Personal Information we collect and process about Contacts through the Service, we act as a processor on behalf of our Members. Mailchimp is not responsible for the privacy or security practices of our Members, which may differ from those set forth in this privacy policy. Please check with individual Members about the policies they have in place. **For purposes of this section, "you" and "your" refer to Contacts.**

A. Information We Collect

The Personal Information that we may collect or receive about you broadly falls into the following categories:

(i) **Information we receive about Contacts from our Members:** A Member may provide Personal Information about you to us through the Service. When a Member uploads their Distribution List or integrates the Service with another website or service (for example, when a Member chooses to connect their e-commerce account with Mailchimp), or when you sign up for a Member's Distribution List on a Mailchimp or other signup form, the Member may provide us with certain contact information or other Personal Information about you such as your name, email address, address, or telephone number. You may have the opportunity to update some of this information by electing to update or manage your preferences via an email you receive from a Member.

(ii) **Information we collect automatically**: When you interact with an email campaign that you receive from a Member or browse or purchase from a Member's connected store, we may collect information about your device and interaction with an email. We use cookies and other tracking technologies to collect some of this information. Our use of cookies and other tracking technologies is discussed more below and in more detail in our Cookie Statement available **here**.

- **Device information:** We collect information about the device and applications you use to access emails sent through our Service, such as your IP address, your operating system, your browser ID, and other information about your system and connection.
- **Usage data:** It is important for us to ensure the security and reliability of the Service we provide. Therefore, we also collect usage data about your interactions with campaigns (and/or emails) sent through the Service, which may include dates and times you access campaigns (and/or emails) and your browsing activities (such as what pages are viewed and which emails are opened). This information also allows us to ensure compliance with our Standard Terms of Use and Acceptable Use Policy, to monitor and prevent service abuse, and to ensure we attain certain usage standards and metrics in relation to our Service. We also collect information regarding the performance of the Service, including metrics related to the deliverability of emails and other electronic communications that our Members send through the Service. This information allows us to improve the content and operation of the Service and facilitate research and perform analysis into the use and performance of the Service.

(iii) **Information we collect from other sources:** From time to time, we may obtain information about you from third-party sources, such as social media platforms, and third-party data providers. We use this information to provide publicly available social media information about you to Members who have enabled the "Social Profiles" feature in their Mailchimp accounts.

B. Use of Personal Information

We may use the Personal Information we collect or receive about you in reliance on our (and where applicable, our Members') legitimate interests for the following purposes:

- To enforce compliance with our Standard Terms of Use and applicable law. This may include utilizing usage data and developing tools and algorithms that help us prevent violations.
- To protect the rights and safety of Members, third parties, or Mailchimp. For example, sometimes we review the content of our Members' email campaigns to make sure they comply with our Standard Terms of Use. To improve that process, we have software that helps us find email campaigns that may violate our Standard Terms of Use. We, or our third-party service provider, may review those particular email campaigns, which may include your contact information. This reduces the amount of spam being sent through our servers and helps us maintain high deliverability.
- To meet legal requirements, including complying with court orders, valid discovery requests, valid subpoenas, and other appropriate legal mechanisms.
- To provide information to representatives and advisors, including attorneys and accountants, to help us comply with legal, accounting, or security requirements.
- To prosecute and defend a court, arbitration, or similar legal proceeding.
- To respond to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- To provide, support and improve the Service. For example, this may include sharing your information with third parties in order to provide and support our Service or to make certain features of the Service available to our Members. When we share Personal Information with third parties, we take steps to protect your information in a manner that is consistent with applicable privacy laws. For further information about how we share information, refer to Section 5 below.
- To perform data analytics projects. Our data analytics projects use data from Mailchimp accounts, including your Personal Information, to provide and improve the Service. We use information, like your purchase history, provided to us by Members, so we can make more informed predictions, decisions, and products for our Members. For example, we use data from Mailchimp accounts to enable product recommendation, audience segmentation, and predicted demographics features for our Members. If you prefer your data not to be used in this manner, you can opt out of data analytics projects at any time by completing this **form** or emailing us at personaldatarequests@mailchimp.com.
- To carry out other business purposes. To carry out other legitimate business purposes, as well as other lawful purposes about which we will notify you.

C. Cookies and Tracking Technologies

We and our third-party partners may use various technologies to automatically collect and store certain device and usage information (as discussed above) when you interact with a Member's email campaign or connected store, and this may include using cookies and similar tracking technologies, such as pixels and web beacons or if a Member is using our Mobile App, we may collect this information through our SDKs deployed on our Members mobile device. For example, we use web beacons in the emails we send on behalf of our Members. When you receive and engage with a Member's campaign, web beacons track certain behavior such as whether the email sent through the Mailchimp platform was delivered and opened and whether links within the email were clicked. Both web beacons and SDKs allow us to collect information such as your IP address, browser, email client type, and other similar data as further described above. We use this information to measure the performance of our Members' email campaigns, and to provide analytics information and enhance the effectiveness of our Service, and for the other purposes described above.

Our use of cookies and other tracking technologies is discussed in more detail in our Cookie Statement available **here**.

D. Your Data Protection Rights

Depending on the country in which you reside, you may have the following data protection rights:

- To access; correct; update; port; delete; restrict or object to our processing of your Personal Information.
- For more information about how you can exercise these rights, please see our Data Subject Requests **form**. You also have the right to complain to a data protection authority about our collection and use of your Personal Information. For more information, please contact your local data protection authority. Contact details for data protection authorities in the EEA are available **here**.

As described above, for much of the Personal Information we collect and process about Contacts through the Service, we act as a processor on behalf of our **Members**. In such cases, if you are a Contact and want to exercise any data protection rights that may be available to you under applicable law or have questions or concerns about how your Personal Information is handled by Mailchimp as a processor on behalf of our individual Members, you should contact the relevant Member that is using the Mailchimp Service, and refer to their separate privacy policies.

If you no longer want to be contacted by one of our Members through our Service, please unsubscribe directly from that Member's newsletter or contact the Member directly to update or delete your data. If you contact us directly, we may either forward

your request to the relevant Member or provide you with the identity of the Member to enable you to contact them directly.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. We may ask you to verify your identity in order to help us respond efficiently to your request.

4. Privacy for Visitors

This section applies to Personal Information that we collect and process when you visit the Mailchimp Sites, and in the usual course of our business, such as in connection with our recruitment, events, sales and marketing activities or when you visit our offices. **In this section, "you" and "your" refer to Visitors.**

A. Information We Collect

(i) **Information you provide to us on the Mailchimp Sites or otherwise:** Our Mailchimp Sites offer various ways to contact us, such as through form submissions, email or phone, to inquire about our company and Service. For example, we may ask you to provide certain Personal Information when you express an interest in obtaining information about us or our Service, take part in surveys, subscribe to marketing, apply for a role with Mailchimp, or otherwise contact us. We may also collect Personal Information from you in person when you attend our events or trade shows, if you visit our offices (where you will be required to register as a visitor and provide us with certain information that may also be shared with our service providers) or via a phone call with one of our sales representatives. You may choose to provide additional information when you communicate with us or otherwise interact with us, and we may keep copies of any such communications for our records.

The Personal Information we collect may include:

- **Business contact information** (such as your name, phone number, email address and country);
- **Professional information** (such as your job title, institution or company);
- **Nature of your communication**;
- **Marketing information** (such as your contact preferences); and
- **Any information you choose to provide to us** when completing any 'free text' boxes in our forms.

(ii) **Information we collect automatically through the Mailchimp Sites:** When you visit our Mailchimp Sites or interact with our emails, we use cookies and similar technologies such as pixels or web beacons, alone or in conjunction with cookies, to collect certain information automatically from your browser or device. In some countries, including countries in the EEA, this information may be considered Personal Information under applicable data protection laws. Our use of cookies and other tracking technologies is discussed more below, and in more detail in our Cookie Statement available **here**.

The information we collect automatically includes:

- **Device information**: such as your IP address, your browser, device information, unique device identifiers, mobile network information, request information (speed, frequency, the site from which you linked to us ("referring page"), the name of the website you choose to visit immediately after ours (called "exit page"), information about other websites you have recently visited and the web browser you used (software used to browse the internet) including its type and language)
- **Usage data**: such as information about how you interact with our emails, Mailchimp Sites, and other websites (such as the pages and files viewed, searches, operating system and system configuration information and date/time stamps associated with your usage).

B. Use of Personal Information

We may use the information we collect through our Mailchimp Sites and in connection with our events and marketing activities (alone or in combination with other data we collect) for a range of reasons in reliance on our legitimate interests, including:

- To provide, operate, optimize, and maintain the Mailchimp Sites.
- To send you marketing information, product recommendations and non-transactional communications (e.g., marketing newsletters, telemarketing calls, SMS, or push notifications) about us, in accordance with your marketing preferences, including information about our products, services, promotions or events as necessary for our legitimate interest in conducting direct marketing or to the extent you have provided your prior consent.
- For recruitment purposes if you have applied for a role with Mailchimp.
- To respond to your online inquiries and requests, and to provide you with information and access to resources or services that you have requested from us.
- To manage the Mailchimp Sites and system administration and security.
- To manage event registrations and attendance, including sending related communications to you.

- To register visitors to our offices for security reasons and to manage non-disclosure agreements that visitors may be required to sign.
- To improve the navigation and content of the Mailchimp Sites.
- To identify any server problems or other IT or network issues.
- To process transactions and to set up online accounts.
- To compile aggregated statistics about site usage and to better understand the preferences of our Visitors.
- To help us provide, improve and personalize our marketing activities.
- To facilitate the security and continued proper functioning of the Mailchimp Sites.
- To carry out research and development to improve our Mailchimp Sites, products and services.
- To conduct marketing research, advertise to you, provide personalized information about us on and off our Mailchimp Sites, and to provide other personalized content based on your activities and interests to the extent necessary for our legitimate interests in supporting our marketing activities or advertising our Service or instances where we seek your consent.
- To carry out other legitimate business purposes, as well as other lawful purposes, such as data analysis, fraud monitoring and prevention, identifying usage trends and expanding our business activities in reliance on our legitimate interests.
- To cooperate with public and government authorities, courts or regulators in accordance with our legal obligations under applicable laws to the extent this requires the processing or disclosure of Personal Information to protect our rights or is necessary for our legitimate interest in protecting against misuse or abuse of our Mailchimp Sites and Service, protecting personal property or safety, pursuing remedies available to us and limiting our damages, complying with judicial proceedings, court orders or legal processes, or responding to lawful requests.

C. Public Information and Third-Party Websites

- **Blog.** We have public blogs on the Mailchimp Sites. Any information you include in a comment on our blog may be read, collected, and used by anyone. If your Personal Information appears on our blogs and you want it removed, contact us **here**. If we are unable to remove your information, we will tell you why.
- **Social media platforms and widgets.** The Mailchimp Sites include social media features, such as the Facebook Like button. These features may collect information about your IP address and which page you are visiting on our Mailchimp Site, and they may set a cookie to make sure the feature functions properly. Social media features and widgets are either hosted by a third party or hosted directly on our Mailchimp Site. We also maintain presences on social

media platforms, including Facebook, Twitter, and Instagram. Any information, communications, or materials you submit to us via a social media platform is done at your own risk without any expectation of privacy. We cannot control the actions of other users of these platforms or the actions of the platforms themselves. Your interactions with those features and platforms are governed by the privacy policies of the companies that provide them.

- **Links to third-party websites.** The Mailchimp Sites include links to other websites, whose privacy practices may be different from ours. If you submit Personal Information to any of those sites, your information is governed by their privacy policies. We encourage you to carefully read the privacy policy of any website you visit.
- **Contests and sweepstakes.** We may, from time to time, offer surveys, contests, sweepstakes, or other promotions on the Mailchimp Sites or through social media (collectively, "Promotions"). Participation in our Promotions is completely voluntary. Information requested for entry may include Personal Information such as your name, address, date of birth, phone number, email address, username, and similar details. We use the information you provide to administer our Promotions. We may also, unless prohibited by the Promotion's rules or law, use the information provided to communicate with you, or other people you select, about our Service. We may share this information with our affiliates and other organizations or service providers in line with this privacy policy and the rules posted for our Promotions.

D. Cookies and Tracking Technologies

We use cookies and similar tracking technologies to collect and use Personal Information about you, including to serve interest-based advertising. For further information about the types of cookies and tracking technologies we use, why, and how you can control them, please see our Cookie Statement available **here**.

E. Other Data Protection Rights

Depending on the country in which you reside, you may have the following data protection rights:

- To access; correct; update; port; delete; restrict or object to our processing of your Personal Information. You can exercise these rights by emailing personaldatarequests@mailchimp.com.
- You may also have the right to complain to a data protection authority about our collection and use of your Personal Information. For more information, please contact your local data protection authority. Contact details for data protection authorities in the EEA are available **here**.

- Similarly, if we have collected and processed your Personal Information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect the processing of your Personal Information conducted in reliance on lawful processing grounds other than consent. You can also contact us at any time to update your marketing preferences (see Section 5. General Information, C. Your Choices and Opt-Outs below).

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. We may ask you to verify your identity in order to help us respond efficiently to your request.

5. General Information

A. How We Share Information

We may share and disclose your Personal Information to the following types of third parties for the purposes described in this privacy policy **(for purposes of this section, "you" and "your" refer to Members, Contacts, and Visitors unless otherwise indicated):**

(i) **Our service providers**: Sometimes, we share your information with our third-party service providers working on our behalf for the purposes described in this privacy policy. For example, companies we've hired to help us provide and support our Service or assist in protecting and securing our systems and services and other business-related functions.

Other examples include analyzing data, hosting data, engaging technical support for our Service, processing payments, and delivering content.

In connection with our Service, we also use a third-party service provider, Twilio, Inc. We use Twilio's API, which allows us to build features into our Mailchimp application to enable us to communicate with our Members through texting and calling, and their "Authy" product, which we use for two-factor authentication for our application. If you are a Member, Twilio may need to collect and process certain Personal Information about you as a controller to provide such services. To learn more about Twilio's privacy practices, please visit **https://www.twilio.com/legal/privacy**.

(ii) **Advertising partners**: We may partner with third-party advertising networks, exchanges, and social media platforms (like Facebook) to display advertising on the Mailchimp Sites or to manage and serve our advertising on other sites, and we may

share Personal Information of Members and Visitors with them for this purpose. We and our third-party partners may use cookies and other similar tracking technologies, such as pixels and web beacons, to gather information about your activities on the Mailchimp Sites and other sites in order to provide you with targeted advertising based on your browsing activities and interests. For more information, please see our Cookie Statement available **here**.

(iii) **Any competent law enforcement body, regulatory body, government agency, court or other third party where** we believe disclosure is necessary (a) as a matter of applicable law or regulation, (b) to exercise, establish, or defend our legal rights, or (c) to protect your vital interests or those of any other person.

(iv) **A potential buyer (and its agents and advisors)** in the case of a sale, merger, consolidation, liquidation, reorganization, or acquisition. In that event, any acquirer will be subject to our obligations under this privacy policy, including your rights to access and choice. We will notify you of the change either by sending you an email or posting a notice on our Mailchimp Site.

(v) **Any other person with your consent.**

B. Legal Basis for Processing Personal Information (EEA and UK Persons Only)

If you are located in the EEA or UK, our legal basis for collecting and using the Personal Information described above will depend on the Personal Information concerned and the specific context in which we collect it.

However, we will normally collect and use Personal Information from you where the processing is in our legitimate interests and not overridden by your data-protection interests or fundamental rights and freedoms. Our legitimate interests are described in more detail in this privacy policy in the sections above titled "Use of Personal Information", but they typically include improving, maintaining, providing, and enhancing our technology, products, and services; ensuring the security of the Service and our Mailchimp Sites; and supporting our marketing activities.

If you are a Member, we may need the Personal Information to perform a contract with you. In some limited cases, we may also have a legal obligation to collect Personal Information from you. If we ask you to provide Personal Information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your Personal Information is

mandatory or not, as well as of the possible consequences if you do not provide your Personal Information.

Where required by law, we will collect Personal Information only where we have your **consent** to do so.

If you have questions or need further information concerning the legal basis on which we collect and use your Personal Information, please contact us using the contact details provided in the "Questions and Concerns" section below.

C. Your Choices and Opt-Outs

Members and Visitors who have opted in to our marketing emails can opt out of receiving marketing emails from us at any time by clicking the "unsubscribe" link at the bottom of our marketing messages.

Also, all opt-out requests can be made by emailing us using the contact details provided in the "Questions and Concerns" section below. Please note that some communications (such as service messages, account notifications, billing information) are considered transactional and necessary for account management, and Members cannot opt out of these messages unless you cancel your Mailchimp account.

D. Our Security

We take appropriate and reasonable technical and organizational measures designed to protect Personal Information from loss, misuse, unauthorized access, disclosure, alteration, and destruction, taking into account the risks involved in the processing and the nature of the Personal Information. For further information about our security practices, please see our Security page available **here**. If you have any questions about the security of your Personal Information, you may contact us at privacy@mailchimp.com.

Mailchimp accounts require a username and password to log in. Members must keep their username and password secure, and never disclose it to a third party. Because the information in a Member's Mailchimp account is private, account passwords are hashed, which means we cannot see a Member's password. We cannot resend forgotten passwords either. We will only provide Members with instructions on how to reset them.

E. International Transfers

(i) **We operate in the United States**

Our servers and offices are located in the United States, so your information may be transferred to, stored, or processed in the United States. While the data protection, privacy, and other laws of the United States might not be as comprehensive as those in your country, we take many steps to protect your privacy, including offering our Members a Data Processing Agreement available **here**.

(ii) **Data transfers from Switzerland, United Kingdom, or the EEA to the United States**

Mailchimp participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. We are committed to subjecting all Personal Information received from EEA member countries, United Kingdom, and Switzerland, respectively, in reliance on each Privacy Shield Framework, to each Framework's applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield website available **here**.

A list of Privacy Shield participants is maintained by the Department of Commerce and is available **here**.

Mailchimp is responsible for the processing of Personal Information we receive under each Privacy Shield Framework and subsequently transfer to a third party acting as an agent on our behalf. We comply with the Privacy Shield Principles for all onward transfers of Personal Information from the EEA, United Kingdom, and Switzerland, including the onward transfer liability provisions.

With respect to Personal Information received or transferred pursuant to the Privacy Shield Frameworks, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge to you) at **https://feedback-form.truste.com/watchdog/request**. Under certain conditions, more fully described on the Privacy Shield website, **here**, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Members located in Switzerland, United Kingdom, and the EEA are subject to our Data Processing Addendum available **here**, as described in our Standard Terms of Use.

(iii) **Members, Contacts and Visitors located in Australia**

If you are a Member, Contact or Visitor who accesses our Service in Australia, this section applies to you. We are subject to the operation of the Privacy Act 1988 **("Australian Privacy Act")**. Here are the specific points you should be aware of:

- As stated in our Acceptable Use Policy available **here**, sensitive personal information is not permitted on Mailchimp's platform and Members are prohibited from importing or incorporating any sensitive personal information into their Mailchimp accounts or uploading any sensitive personal information to Mailchimp's servers.
- Please note that if you do not provide us with your Personal Information or if you withdraw your consent for us to collect, use and disclose your Personal Information, we may be unable to provide the Service to you.
- Where we collect Personal Information of our Visitors, the Personal Information we ask you to provide will be information that is reasonably necessary for, or directly related to, one or more of our functions or activities. Please see **Section 4** of this privacy policy for examples of the types of Personal Information we may ask Visitors to provide.
- Where we say we assume an obligation about Personal Information, we will also require our contractors and subcontractors to undertake a similar obligation.
- We will not use or disclose Personal Information for the purpose of our direct marketing to you unless:
    - you have consented to receive direct marketing;
    - you would reasonably expect us to use your personal details for marketing; or
    - we believe you may be interested in the material but it is impractical for us to obtain your consent.

You may opt out of any marketing materials we send to you through an unsubscribe mechanism. If you have requested not to receive further direct marketing messages, we may continue to provide you with messages that are not regarded as "direct marketing" under the Australian Privacy Act, including changes to our terms, system alerts, and other information related to your account as permitted under the Australian Privacy Act and the Spam Act 2003 (Cth).

- Our servers are located in the United States. In addition, we or our subcontractors may use cloud technology to store or process Personal Information, which may result in storage of data outside Australia. It is not practicable for us to specify in advance which country will have jurisdiction over this type of offshore activity. All of our subcontractors, however, are required to

comply with the Australian Privacy Act in relation to the transfer or storage of Personal Information overseas.

- We may also share your Personal Information outside of Australia to our business operations in other countries. While it is not practicable for us to specify in advance each country where your Personal Information may be disclosed, typically we may disclose your Personal Information to the United States, Canada and the European Union.
- You may access the Personal Information we hold about you. If you wish to access your Personal Information, please contact us directly by emailing us at personaldatarequests@mailchimp.com. We will respond to all requests for access within a reasonable time.

If you think the information we hold about you is inaccurate, out of date, incomplete, irrelevant, or misleading, we will take reasonable steps, consistent with our obligations under the Australian Privacy Act, to correct that information upon your request. If you find that the information we have is not up to date or is inaccurate or incomplete, please contact us in writing at dpo@mailchimp, so we can update our records. We will respond to all requests for correction within a reasonable time.

- If you are unsatisfied with our response to a privacy matter, you may consult either an independent advisor or contact the Office of the Australian Information Commissioner for additional help. We will provide our full cooperation if you pursue this course of action.

F. Retention of Data

We retain Personal Information where we have an ongoing legitimate business or legal need to do so. Our retention periods will vary depending on the type of data involved, but, generally, we'll refer to these criteria in order to determine retention period:

- Whether we have a legal or contractual need to retain the data.
- Whether the data is necessary to provide our Service.
- Whether our Members have the ability to access and delete the data within their Mailchimp accounts.
- Whether our Members would reasonably expect that we would retain the data until they remove it or until their Mailchimp accounts are closed or terminated.

When we have no ongoing legitimate business need to process your Personal Information, we will either delete or anonymize it or, if this is not possible (for example, because your Personal Information has been stored in backup archives), then we will securely store your Personal Information and isolate it from any further processing until deletion is possible.

G. California Privacy

The California Consumer Privacy Act ("CCPA") provides consumers with specific rights regarding their Personal Information. You have the right to request that businesses subject to the CCPA (which may include our Members with whom you have a relationship) disclose certain information to you about their collection and use of your Personal Information over the past 12 months. In addition, you have the right to ask such businesses to delete Personal Information collected from you, subject to certain exceptions. If the business sells Personal Information, you have a right to opt-out of that sale. Finally, a business cannot discriminate against you for exercising a CCPA right.

When offering services to its Members, Mailchimp acts as a "service provider" under the CCPA and our receipt and collection of any consumer Personal Information is completed on behalf of our Members in order for us to provide the Service. Please direct any requests for access or deletion of your Personal Information under the CCPA to the Member with whom you have a direct relationship.

Consistent with California law, if you choose to exercise your applicable CCPA rights, we won't charge you different prices or provide you a different quality of services. If we ever offer a financial incentive or product enhancement that is contingent upon you providing your Personal Information, we will not do so unless the benefits to you are reasonably related to the value of the Personal Information that you provide to us.

H. Do not Track

Certain state laws require us to indicate whether we honor "Do Not Track" settings in your browser. Mailchimp adheres to the standards set out in this Privacy Policy and does not monitor or follow any Do Not Track browser requests.

I. Changes to this Policy

We may change this privacy policy at any time and from time to time. The most recent version of the privacy policy is reflected by the version date located at the top of this privacy policy. All updates and amendments are effective immediately upon notice, which we may give by any means, including, but not limited to, by posting a revised version of this privacy policy or other notice on the Mailchimp Sites. We encourage you to review this privacy policy often to stay informed of changes that may affect you. Our electronically or otherwise properly stored copies of this privacy policy are each deemed to be the true, complete, valid, authentic, and enforceable copy of the version

of this privacy policy that was in effect on each respective date you visited the Mailchimp Site.

J. Questions & Concerns

If you have any questions or comments, or if you have a concern about the way in which we have handled any privacy matter, please use our **contact form** to send us a message. You may also contact us by postal mail or email at:

For EEA, Swiss and UK Residents:

For the purposes of EU data protection legislation, The Rocket Science Group LLC d/b/a Mailchimp is the controller of your Personal Information. Our Data Protection Officer can be contacted at **dpo@mailchimp.com**.

For any other Residents:

The Rocket Science Group LLC d/b/a Mailchimp
Attn. Privacy Officer
privacy@mailchimp.com
675 Ponce de Leon Ave NE, Suite 5000
Atlanta, GA 30308 USA

LEGAL

Data Processing Addendum

In this document

This Data Processing Addendum ("**DPA**") is incorporated into, and is subject to the terms and conditions of, the Agreement between The Rocket Science Group LLC d/b/a Mailchimp (together with its Affiliates, "**Mailchimp**") and the customer entity that is a party to the Agreement ("**Customer**" or "**you**").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the "Agreement" shall include this DPA (including the SCCs (where applicable), as defined herein).

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 **Standard Terms of Use**, or other written or electronic agreement, which govern the provision of the Service to Customer, as such terms or agreement may be updated 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 via the Service, as more particularly described in this DPA.

"**Data Protection Laws**" means all data protection laws and regulations applicable to a party's processing of Customer Data under the Agreement, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.

"**EU Data Protection Law**" means all data protection laws and regulations applicable to Europe, including (i) 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**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iii) in respect of the United Kingdom ("**UK**") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union).

"**Europe**" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

"**Non-EU Data Protection Laws**" means the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018.

"**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.

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles).

"**SCCs**" means the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by Mailchimp.

"**Sensitive Data**" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or

religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

"**Service Data**" means any data relating to the Customer's use, support and/or operation of the Service, including information relating to volumes, activity logs, frequencies, bounce rates or other information regarding emails and other communications Customer generates and sends using the Service.

"**Sub-processor**" means any processor engaged by Mailchimp or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of Mailchimp but shall exclude Mailchimp employees or consultants.

The terms "**personal data**", "**controller**", "**data subject**", "**processor**" and "**processing**" shall have the meaning given to them under Data Protection Laws or if not defined thereunder, the GDPR, and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

2. Roles and Responsibilities

2.1 **Parties' roles**. If EU Data Protection Law or the LGPD applies to either party's processing of Customer Data, the parties acknowledge and agree that with regard to the processing of Customer Data, Customer is the controller and Mailchimp is a processor acting on behalf of Customer, as further described in Annex A (Details of Data Processing) of this DPA.

2.2 **Purpose limitation**. Mailchimp shall process Customer Data only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing ("Permitted Purposes"). The parties agree that the Agreement sets out 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 the parties.

2.3 **Prohibited data**. Customer will not provide (or cause to be provided) any Sensitive Data to Mailchimp for processing under the Agreement, and Mailchimp will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

2.4 **Customer compliance**. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Customer Data and any processing instructions it issues to Mailchimp; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Mailchimp to process Customer Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Service, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices.

2.5 **Lawfulness of Customer's instructions**. Customer will ensure that Mailchimp's processing of the Customer Data in accordance with Customer's instructions will not cause Mailchimp to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Mailchimp shall promptly notify Customer in writing, unless prohibited from doing so under EU Data Protection Laws, if it becomes aware or believes that any data processing instruction from Customer violates the GDPR or any UK implementation of the GDPR.

3. Sub-processing

3.1 **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 available **here**. Mailchimp shall notify Customer if it adds or removes Sub-processors at least 10 days prior to any such changes if Customer opts in to receive such notifications by clicking **here**.

3.2 **Sub-processor obligations**. Mailchimp shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Mailchimp to breach any of its obligations under this DPA.

4. Security

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

4.2 **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).

4.3 **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 Service meets 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 Service provided to Customer.

4.4 **Security Incident response**. Upon becoming aware of a Security Incident, Mailchimp shall: (i) notify Customer without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. Mailchimp's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by Mailchimp of any fault or liability with respect to the Security Incident.

4.5 **Customer responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Service.

5. Security Reports and Audits

5.1 **Audit rights**. Mailchimp shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA.

Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 5.1 and where applicable, the SCCs) and any audit rights granted by Data Protection Laws, by instructing Mailchimp to comply with the audit measures described in Sections 5.2 and 5.3 below.

5.2 **Security reports**. Customer acknowledges that Mailchimp is regularly audited against SSAE 16 and PCI standards by independent third party auditors and internal auditors respectively. Upon written request, Mailchimp shall supply (on a confidential basis) a summary copy of its most current 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.

5.3 **Security due diligence**. In addition to the Report, Mailchimp shall respond to all reasonable requests for information made by Customer to confirm Mailchimp's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to privacy@mailchimp.com, provided that Customer shall not exercise this right more than once per calendar year.

6. International Transfers

6.1 **Data center locations**. Customer acknowledges that Mailchimp may transfer and process Customer Data to and in the United States and anywhere else in the world where Mailchimp, its Affiliates or its Sub-processors maintain data processing operations. Mailchimp shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws.

6.2 **European Data transfers**. To the extent that Mailchimp is a recipient of Customer Data protected by EU Data Protection Laws ("EU Data"), the parties agree that Mailchimp makes available the mechanisms listed below:

- (a) **Privacy Shield**: For as long as Mailchimp is self-certified to the Privacy Shield: (i) the parties acknowledge and agree that Mailchimp will be deemed to provide adequate protection (within the meaning of applicable EU Data Protection Laws) for EU Data by virtue of having self-certified its compliance with Privacy Shield; (ii) Mailchimp agrees to process EU Data in compliance with the Privacy Shield Principles; and (iii) if Mailchimp is unable to comply with this requirement, Mailchimp shall inform Customer.
- (b) **SCCs**: Mailchimp agrees to abide by and process EU Data in compliance with the SCCs, which are incorporated in full by reference and form an integral

part of this DPA. For the purposes of the SCCs: (i) Mailchimp agrees that it is the "data importer" and Customer is the "data exporter" under the SCCs (notwithstanding that Customer may itself be an entity located outside the EU); (ii) Annexes A and B of this DPA shall replace Appendixes 1 and 2 of the SCCs, respectively; and (iii) Annex C shall form Appendix 3 of the SCCs. The parties further agree that the SCCs will apply to Customer Data that is transferred via the Service from Europe to outside Europe, either directly or via onward transfer, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Law); and (b) not covered by Mailchimp's Privacy Shield certification.

7. Return or Deletion of Data

7.1 **Deletion on termination**. 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, except 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, protect from any further processing and eventually delete in accordance with Mailchimp's deletion policies, except to the extent required by applicable law.

8. Data Subject Rights and Cooperation

8.1 **Data subject requests**. As part of the Service, Mailchimp provides Customer with a number of self-service features, that Customer may use to retrieve, correct, delete or restrict the use of Customer Data, which Customer may use to assist it in connection with its obligations under the Data Protection Laws with respect to responding to requests from data subjects via Customer's account at no additional cost. In addition, Mailchimp shall, taking into account the nature of the processing, provide reasonable additional assistance to Customer to the extent possible to enable Customer to comply with its data protection obligations with respect to data subject rights under Data Protection Laws. In the event that any such request is made to Mailchimp directly, Mailchimp shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact Customer) or legally required, without Customer's prior authorization. If Mailchimp is required to respond to such a request, Mailchimp shall promptly notify Customer and provide Customer with a copy of the request unless Mailchimp is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent Mailchimp

from responding to any data subject or data protection authority requests in relation to personal data for which Mailchimp is a controller.

8.2 **Subpoenas and court orders**. 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.

8.3 **Data protection impact assessment**. To the extent required under applicable Data Protection Laws, Mailchimp shall (taking into account the nature of the processing and the information available to Mailchimp) provide all reasonably requested information regarding the Service to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. Mailchimp shall comply with the foregoing by: (i) complying with Section 5 (Security Reports and Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

9. Jurisdiction-Specific Terms

To the extent Mailchimp processes Customer Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex D, then the terms specified in Annex D with respect to the applicable jurisdiction(s) ("Jurisdiction-Specific Terms") apply in addition to the terms of this DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and any other terms of this DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms' applicability to Mailchimp.

10. Limitation of Liability

10.1 Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

10.2 Any claims made against Mailchimp or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. Relationship with the Agreement

11.1 This DPA shall remain in effect for as long as Mailchimp carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 7.1 above).

11.2 The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Service.

11.3 In the event of any conflict or inconsistency between this DPA and the Mailchimp Standard Terms of Use, the provisions of the following documents (in order of precedence) shall prevail: (a) SCCs; then (b) this DPA; and then (c) the Mailchimp Standard Terms of Use.

11.4 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.5 Notwithstanding anything to the contrary in the Agreement (including this DPA), Mailchimp shall have a right to collect, use and disclose Service Data for its legitimate business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, develop, optimize and maintain the Service; (iii) to investigate fraud, spam, wrongful or unlawful use of the Service; and/or (iv) as required by applicable law.

To the extent any such Service Data is considered personal data under Data Protection Laws, Mailchimp shall be responsible for and shall process such data in accordance with the **Mailchimp Privacy Policy** and Data Protection Laws. For the avoidance of doubt, this DPA shall not apply to Service Data.

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

11.7 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.

Annex A – Details of Data Processing

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

(b) **Duration of processing**: Mailchimp will process Customer Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

(c) **Purpose of processing**: Mailchimp shall only process Customer Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement.

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

(e) **Categories of data subjects**: (i) Members; and (ii) Contacts, each as defined in the Mailchimp Privacy Policy.

(f) **Types of Customer Data**: Customer may upload, submit or otherwise provide certain personal data to the Service, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data:

- **Members**: 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);
- **Contacts**: 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 publicly 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).

(g) **Sensitive Data**: Mailchimp does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service.

(h) **Processing Operations**: Customer Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain and improve the Service provided to Customer pursuant to the Agreement; and/or
- Disclosures in accordance with the Agreement and/or as compelled by applicable law.

Annex B – Security Measures

The Security Measures applicable to the Service are described **here** (as updated from time to time in accordance with Section 4.3 of this DPA).

Annex C

All defined terms used in this Annex C shall have the meaning given to them in the SCCs unless otherwise defined in this Annex.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "DPA" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated and "Agreement" shall have the meaning given to it in the DPA.

Clause 5(a): Suspension of data transfers and termination

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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 Clauses.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 5 (Security Reports and Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not to limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 3 (Sub-processing) of the DPA.

Annex D - Jurisdiction-Specific Terms

Europe:

1. Objection to Sub-processors. Customer may object in writing to Mailchimp's appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with Section 3.1 of DPA, 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 a commercially reasonable resolution. If no such resolution can be reached, Mailchimp will, at its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

California:

1. The definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "personal data" includes "Personal Information"; in each case as defined under CCPA.
2. For this "California" section of Annex D only, "Mailchimp Services" means the suite of marketing tools and insights available for Mailchimp Customers to use, including without limitation, email campaign management, advertisements, and direct mailings and other related digital communications, analytics and tools

made available through the Mailchimp online marketing platform, as may be further described in the App and/or on the Mailchimp Site.

3. For this "California" section of Annex D only, "Permitted Purposes" shall include processing Customer Data only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, or as otherwise may be permitted for "service providers" under the CCPA.
4. Mailchimp's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, apply to Consumer's rights under the CCPA.
5. Notwithstanding any use restriction contained elsewhere in this DPA, Mailchimp shall process Customer Data only to perform the Mailchimp Services, for the Permitted Purposes and/or in accordance with Customer's documented lawful instructions, except where otherwise required by applicable law.
6. Mailchimp may de-identify or aggregate Customer Data as part of performing the Service specified in this DPA and the Agreement.
7. Where Sub-processors process the personal data of Customer contacts, Mailchimp takes steps to ensure that such Sub-processors are Service Providers under the CCPA with whom Mailchimp has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA's definition of "sale". Mailchimp conducts appropriate due diligence on its Sub-processors.

Canada:

1. Mailchimp takes steps to ensure that Mailchimp's Sub-processors, as described in Section 3 (Sub-processing) of the DPA, are third parties under PIPEDA, with whom Mailchimp has entered into a written contract that includes terms substantially similar to this DPA. Mailchimp conducts appropriate due diligence on its Sub-processors.
2. Mailchimp will implement technical and organizational measures as set forth in Section 4 (Security) of the DPA.

Effective January 1, 2020