Marin Software Data Processing Addendum

Date Last Updated: October 9, 2020

This Data Processing Addendum ("**DPA**") is referred to and forms part of the Marin Software Subscription Services Terms of Use and Marin Software Subscription Services Order Form ("**Agreement**") between Marin Software and You. Where Personal Data processed under the Agreement is subject to Applicable Data Protection Law, Marin Software and You may enter into this Marin Software Data Processing Agreement which incorporates by reference the European Commission Decision C(2010)593 Standard Contractual Clauses (processors) (the "**EU Model Clauses**").

1. Data Protection.

1.1. *Definitions:* In this DPA, the following terms shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Law; and

(b) "**Applicable Data Protection Law**" shall mean: (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(c) "**Personal Data**" shall mean any data related to an identified or identifiable individual natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to its physical, physiological, mental, economic, cultural or social identity.

1.2. *Relationship of the parties:* You (the controller) appoint Marin Software as a processor to process the Personal Data described in Appendix 1 to Schedule A attached hereto. Each party shall comply with this DPA and any obligations that apply to it under Applicable Data Protection Law.

1.3. *Prohibited data:* You shall not disclose (and shall not permit any data subject to disclose) any special categories of Personal Data to Marin Software for processing that are not expressly disclosed in Appendix 1 to Schedule A.

1.4. *Purpose limitation:* Marin Software shall process the Personal Data as a processor for the purposes described Schedule A and as necessary to perform its obligations under the Agreement and strictly in accordance with Your documented instructions (the "**Permitted Purpose**", except where otherwise required by any EU (or any EU Member State) law applicable to You. In no event shall Marin Software process any Personal Data for its own purposes or those of any third party.

1.5. *International transfers:* Marin Software shall not transfer the Personal Data (nor permit the Personal Data to be transferred) outside of the European Economic Area ("**EEA**") unless (i) it has first obtained Your prior written consent; and (ii) it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Personal Data to a recipient

in a country that the European Commission has decided provides adequate protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission. You consent to Marin Software processing all Subscriber Data, including Personal Data, in the United States of America.

1.6. *Confidentiality of processing:* Marin Software shall ensure that any person that it authorises to process the Personal Data (including Marin Software's staff, agents and subcontractors) (an "**Authorized Person**") shall be subject to a strict duty of confidentiality (whether a contractual or a statutory duty), and shall not permit any person to process the Personal Data who is not under such a duty of confidentiality. Marin Software shall ensure that all Authorised Persons process the Personal Data only as necessary for the Permitted Purpose.

1.7. *Security:* Marin Software shall implement appropriate technical and organizational measures to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Personal Data (a "**Security Incident**"). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:

(a) the pseudonymisation and encryption of Personal Data where possible;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Subscription Services;
(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

1.8. *Subcontracting:* Marin Software shall not subcontract any processing of the Personal Data to a third party subcontractor without Your prior written consent. Notwithstanding this, You consent to Marin Software engaging third party subprocessors to process the Personal Data provided that: (i) Marin Software provides at least 30 days' prior notice of the addition of any Subprocessor (including details of the processing it performs or will perform), which may be given by providing notice to the notice recipients in the Agreement; (ii) Marin Software imposes data protection terms on any subprocessor it appoints that protect the Personal Data to the same standard provided for by this Clause; and (iii) Marin Software remains fully liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. A list of approved subprocessors as at the date of this DPA is attached in Appendix 1 to Schedule A, and Marin Software shall maintain and provide updated copies of this list to Subscriber when it adds or removes a subprocessor in accordance with this Clause. If You refuse to consent to Marin Software's appointment of a subprocessor on reasonable grounds relating to the protection of the Personal Data, then either Marin Software will not appoint the subprocessor or You may elect to suspend or terminate the Agreement upon 30 days' written notice to Marin Software.

1.9. *Cooperation and data subjects' rights:* Marin Software shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to You (at its own expense) to enable You to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Personal Data. In the event that any such request, or complaint is made directly to Marin Software, Marin Software shall promptly inform You providing full details of the same.

1.10. *Data Protection Impact Assessment:* If Marin Software believes, or becomes aware that its processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform You and provide You with all such reasonable and timely assistance as You may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

1.11. *Security incidents:* Upon becoming aware of a Security Incident, Marin Software shall inform You without undue delay and provide timely information and cooperation as You may require in order for You to fulfil Your data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Marin Software shall further take commercially reasonable measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep You up-to-date about all developments in connection with the Security Incident.

1.12. *Deletion or return of Personal Data:* Upon termination or expiry of this DPA, Marin Software shall (at Your election) destroy or return to You all Personal Data in its possession or control (including any Personal Data subcontracted to a third party for processing). This requirement shall not apply to the extent that Marin Software is required by any EU (or any EU Member State) law to retain some or all of the Personal Data, in which event Marin Software shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

1.13. *Audit:* Marin Software shall permit You to audit Marin Software's compliance with this DPA, and shall make available to You all information, systems and staff reasonably necessary for You to conduct such audit. Marin Software acknowledges that You may enter its premises for the purposes of conducting this audit, provided that You provide reasonable prior notice of Your intention to audit, conducts Your audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Marin Software's operations. You will not exercise its audit rights more than once in any 12 calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) if You believes a further audit is necessary due to a Security Incident suffered by Marin Software.

Appendix 1 to the Standard Contractual Clauses

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

1. Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

You are the data exporter that has purchased the Subscription Services under the Agreement.

2. Data importer

The data importer is Marin Software providing the Subscription Services under the Agreement.

3. Data subjects

The personal data transferred concern the following categories of data subjects: Internet users accessing the data exporter's website and/or using the data exporter's online services.

Authorized users of the Subscription Services.

4. Categories of data

The personal data transferred concern the following categories of data.

When using Marin Tracker (Tracking Pixel):

The Marin Tracker Pixel consists of two JavaScript snippets. The first snippet, called the Landing Page Tag, can be installed on all pages of the Data Exporter's (or advertiser) website. It tracks incoming traffic by logging the HTTP referrer URL. The other snippet is a Conversion Tag, and may be installed on conversion pages only. This tracks conversion events from paid click campaigns

The Marin Conversion tag is used track conversion events. The Marin Tracker conversion captures both the time and the date of action 1 and 2's (click and conversion data) so that revenue and conversions can be attributed back to Data Exporter's (or advertiser) keywords and/or creatives.

The Marin Landing Page Tag tracks all incoming traffic to the Data Exporter's (or advertiser) site by logging the HTTP referrer URL. In the context of paid click campaigns, the referrer URL is known as the Landing Page URL.

When using the Marin Tracker landing page tag further information can be captured. The landing page tag will be able to capture this information not only for visits from PPC clicks but for all visitors reaching a page on your site. The tag also stores a randomly generated UUID which is required to track a visitors' conversion back to the original arrival on a landing page (and thus the click on an ad).

Marin Tracker collects the following data from the advertiser's landing web page:

- IP address of Internet user (these data are anonymized by replacing the last octet with a "1" for all IP Addresses originating in the European Economic Area)
- Current time stamp
- URL of the web site from which the Internet user was referred to the advertiser's web page
- URL of the advertiser's web sites the Internet user is visiting
- Operating system of the device used by the Internet user
- Browser type and version of the Internet user's device
- Search engine of the Internet user
- Keyword searched for by the Internet user
- Unique user identifier generated by Marin Tracker

Marin Tracker collects the following data from the advertiser's thank you page:

- Conversion type-ID
- Order ID (transmission is optional)
- Revenue (transmission is optional)

- current timestamp
- URL of the Website, from which the User was directed to the advertiser's site
- URL of the advertiser's website
- Operating system of the device the Internet user is using
- Type of browser and browser version of the device the Internet user is using
- Search engine the Internet user is using
- Keyword searched for from the Internet user
- Unique User ID generated by Marin Tracker

MarinOne: Application user data: email address, first and surname, phone number, job title, employment mailing address.

5. Special categories of data (if appropriate): None

6. Processing operations

The following processing operations apply as below:

1. For Marin Software applications (MarinOne Search and Social):
   a. Marin Software processes the personal data of the Subscription Services users in its application servers, and through the use of a third-party customer relationship management software as a service provider.
   b. Marin Software uses the Subscription Services user's email addresess as logon credentials for the Subscription Services. These personal data are stored in Marin Software's data center located in Las Vegas Nevada U.S.A.
   c. Marin Software provides real-time training sessions for customers of the Subscription Services on a voluntary basis. To faciliate registrations for such trainings, Marin Software uses a third-party to collect certain registration details such as email address of the attendee and first and last names.
   d. Marin Software uses a third-party email and alert services delivery provider for emailed reports and alerts sent from the Subscription Services. This subprocessor has access to email addresses and email message contents sent from the data importer's applications. These data are maintained on the subprocessor's data centers located in the USA.

2. For Marin Software customers that use Marin Tracker, the following additional processing occurs:
   a. When an Internet user clicks on the web site of the data exporter, a tracking pixel (Marin Tracker) provided by Marin Software, is installed on the web site of the data exporter (or their advertiser customers), collects personal data of the Internet user as described above.
   b. Those data are transferred from the web site of the data exporter (or advertiser) to the delivery content network server (the **"DCN"**) of Amazon CloudFront and then routed to Marin Software's front-end servers located in Germany (the "**Marin Servers**").
   c. The Marin Servers obfuscate the last octet of the internet protocol addresses and send a cookie with a unique identifier to the Internet user's web-browser. The Marin Servers send the anonymized IP address and other collected personal data to the data importer's primary data center located in Las Vegas, Nevada, U.S.A.
   d. The data transferred from the Internet user's browser to the DCN and then the Marin Servers are encrypted via https (provided that the data exporter's website uses https). The data importer encrypts all data via ssh when transmitting to, or within the data center in Las Vegas.
   e. The DCN receives the data directly from the data exporter's web site. Upon receipt the DCN decrypts the data, determines the correct recipient of the data, re-encrypts the data and transmits the re-encrypted data to the Marin Servers.
   f. The DCN makes no further use or processing of the encrypted personal data, except the following: Amazon CloudFront analyzes the Internet user's IP addresses using heuristics to ensure that only "valid" IP addresses are accessing the data exporter's website(s). Amazon CloudFront performs this analysis in their data centers located in the U.S.A.

3. Marin Software uses the following entities as subprocessors under this Agreement.

Name	Purpose	Location	Transfer Mechanism	Data Processed
Salesforce Incorporated	CRM provider	The Landmark @ One Market, Suite 300, San Francisco, CA 94105	EU Standard Contractual Clauses. Trust and Compliance documentation located at: https://help.salesforce.com/articleView?id=Trust-and-Compliance-Documentation&language=en_US&type=1	Customer contact and data which includes: first name, surname, employment address, employment email address, phone number, and job title.
Marketo Inc.	Marketing data provider.	901 Mariners Island Blvd., Suite 500, San Mateo, CA 94404 USA	EU Model Clauses and GDPR Addendum executed between Marin Software and Marketo.	Customer contact and data which includes: first name, surname, employment address, employment email address, phone number, and job title
Amazon Webservices	Provider of data center services in Europe for Marin Software's front-end data servers.	410 Terry Ave., North, Seattle, WA 98109 USA	EU Standard Contractual Clauses.. Information on their compliance program and certifications can be found here: https://aws.amazon.com/compliance/	Application user data: first name, surname, Marin Tracker data.
Amazon CloudFront	Provider of Content Delivery Services for data transferred from Marin Software's front-end servers.	410 Terry Ave., North, Seattle, WA 98109 USA	EU Standard Contractual Clauses.. Information on their compliance program and certifications can be found here: https://aws.amazon.com/compliance/	Marin Tracker data.
Google LLC	Marin Software uses G-Suite which includes email services, document management and storage services, and document processing services.	1600 Amphitheater Parkway, Mountain View, CA 94043 USA	EU Standard Contractual Clauses.	Customer contact and data which includes: first name, surname, employment address, employment email address, phone number, and job title.
SendGrid	Email and alert service delivery service provider for Marin Social and MarinOne.	1801 California Street, Suite 500, Denver Colorado 80202, USA	EU Standard Contractual Clauses. Privacy documentation located at: https://sendgrid.com/policies/privacy/services-privacy-policy/	Limited application user data: email address, and first name, surname.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Unauthorized persons are prevented from gaining access to the data processing systems with which the transferred data are processed or used (**physical access control**):
    a. Marin Software requires its co-location facility partners to restrict physical access to those with prior authorization and picture identification. Marin Software's data center is co-located in an SSAE No. 18 audited Tier IV Gold facility. Only individuals authorized by Marin Software can access Marin Software's equipment. Marin Software requires its providers to enforce verification of Marin Software service requests; providers may not attempt to gain any sort of access to Marin Software's systems without written instructions from Marin Software. Beyond this, no external physical connections to Marin Software systems are allowed including keyboards, displays and network monitoring systems.
2. Data processing systems are prevented from being used without authorization (**logical access control**):
    a. Data processing systems are prevented from being used without authorization. Administrative access to Marin Software's servers are restricted to trained and authorized members of the data importer's staff. Administrative access to the Marin Software application are strictly controlled by the data importer to authorized individuals on a need-to-know basis. Remote administrative access is only available via cryptographically secure connections.
    b. Marin Software uses a strong password policy and two-factor authentication for access to all corporate computing assets. Remote access to the data importer's corporate networks are via secure VPN. The data importer stores all data behind its firewalls and employs advanced alerting systems to detect unauthorized access. All access attempts are logged for the Marin Software's applications and corporate systems.
3. Persons entitled to use a personal data processing system can gain access only to such data as they are entitled to accessing in accordance with their access rights, and, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorization (**data access control**):
    a. Marin Software uses a role-based provisioning process when providing access to the Marin Software applications and its third party customer relationship management software (the "**CRM**"). Only individuals with a "need-to-know" basis are provided access to customer data in the Marin Software applications and the CRM.
    b. The data imp Marin Software orter maintains a strict back-ground check process for all staff and a tightly controlled termination process for revoking access. User provisioning for corporate systems are reviewed twice annually. The data importer's customers control the user provisioning for their users in the Marin Software applications.
4. Personal data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (**transmission control**):
    a. Personal data cannot be read, copied, modified, or removed without authorization during electronic transmission, transportation, or storage. All personal data in the Marin Software applications is protected behind secure firewalls and all access to the data storage is logged in the Marin Software applications and in the server logs. Marin Software uses alerting software to provide alerts for any unauthorized access. Login credentials to the Marin Software application are hashed in storage and encrypted in transmission.
5. It is possible to check and establish whether and by whom personal data have been entered into, modified in, or removed from data processing systems (**input control**):
    a. It is possible to retroactively examine and establish whether and by whom personal data have been process, accessed, or modified. The Marin Software applications and CRM systems contain robust logging features which identify when data are access, modified, or deleted. The data importer and its customers review these logs regularly.

6. Personal data processed on the basis of commissioned processing are processed strictly in accordance with the instructions of the data controller (**job control**):
    a. Marin Software only processes personal data based on the instructions of the data exporter as described in the applicable services agreement between the parties.
7. Personal data are protected against accidental destruction or loss (**availability control**):
    a. Marin Software maintains appropriate and regular back-up procedures daily to prevent accidental destruction of loss of personal data. Data are backed up at regular intervals throughout the day and every complete data back-up are performed every 24 hours.
8. Personal Data collected for different purposes or different subscribers can be processed separately (**separation control**):
    a. Marin Software maintains logical technical separation in its databases to prevent the co-mingling of customer's data. Personal data that are stored in the data importer's data center are hashed in storage and encrypted in transmission. Additionally, the data importer provides all internet users the ability to opt-out of being tracked by the Marin Tracker pixel. The opt-outs are located on the website of the data importer at: http://www.marinsoftware.com/privacy/marin-tracker-opt-out.