Marin Software Data Processing Addendum

Date Last Updated: September 30, 2021

This Data Processing Addendum ("**DPA**") supplements and forms part of the Marin Software Subscription Services Terms of Use available at https://www.marinsoftware.com/terms-of-use, as updated from time to time, and the Marin Software Subscription Services Order Form or other agreement between Marin Software and You ("**Agreement**"). When Personal Data processed under the Agreement is subject to Applicable Data Protection Laws, this DPA and the Standard Contractual Clauses attached to this DPA (the "**EU Standard Contractual Clauses**") shall apply**.**

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 Annex 1, Section A to the EU Standard Contractual Clauses that are attached to this DPA. 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 Annex III to the EU Standard Contractual Clauses that are attached to this DPA, 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.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:
  (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I, Section A (hereinafter each 'data exporter'), and
  (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')
  have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I, Section B.
(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  (v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

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

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I, Section C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts

ANNEX I

Section A. LIST OF PARTIES

Data exporter(s): Subscriber to Marin Software's services

Subscriber contact information: As provided in the applicable Marin Software Subscription Services Order Form or other agreement between Marin Software and the Subscriber

Role (controller/processor): Controller

Data importer:

Name: Marin Software Incorporated

Address: 123 Mission Street, 27th Floor, San Francisco, CA 94105 USA

Contact person's name, position and contact details: General Counsel – legal@marinsoftware.com

Activities relevant to the data transferred under these Clauses: Provision of Marin's Software subscription services to Subscriber

Role (controller/processor): Processor

Section B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

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.

Categories of personal data transferred:

The personal data transferred concern the following categories of data.

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

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 to 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

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous for the term of the governing agreement.

Nature of the processing

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.

Purpose(s) of the data transfer and further processing

None.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Personal data are retained for the term of the governing agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Section C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Irish Data Protection Authority

ANNEX II

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

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.

ANNEX III

LIST OF SUB-PROCESSORS

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.
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.
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.