DATA PROCESSING ADDENDUM

INSTRUCTIONS

Latest Update: October 03, 2022

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, and 3.

2. This DPA has been pre-signed on behalf of Sitetracker.

3. To complete this DPA, Customer must:

    a. Complete the Customer Name and Customer Address Section on page 2.

    b. Complete the information in the signature box and sign on page 10.

    c. Verify that the information on Schedule 2 ("Details of the Processing") accurately reflects the subjects and categories of data to be processed.

    d. Send the completed and signed DPA to Sitetracker at privacy@sitetracker.com.

Upon Sitetracker's receipt of the validly completed DPA at this email address, this DPA will become legally binding.

Signature of this DPA on page 10 shall be deemed to constitute signature and acceptance of the 2021 Standard Contractual Clauses (Module II - "Controller to Processor") and(or) Standard Contractual Clauses (UK) incorporated herein, including their Appendices, as applicable.

HOW THIS DPA APPLIES:

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Sitetracker entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with Sitetracker pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Sitetracker entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity that is a party to the Agreement execute this DPA.

If the Customer entity signing the DPA is not a party to an Order Form nor a Master Subscription and Services Agreement directly with Sitetracker, but is instead a customer indirectly via an authorized reseller of services provided by Sitetracker, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether an amendment to its agreement with that reseller is required.

In the event of any conflict or inconsistency between this DPA and any other agreement between Customer and Sitetracker (including, without limitation, the Agreement or any data processing addendum to the Agreement), the terms of this DPA shall control and prevail.

DATA PROCESSING ADDENDUM

Customer Full Legal Name:	
Customer Address:	

This Data Processing Addendum, including its Schedules and appendices attached thereto, (this "**DPA**") forms part of the Master Subscription and Services Agreement between Sitetracker, Inc. ("**Sitetracker**") and Customer for the purchase of services from Sitetracker (the "**Agreement**") to document the parties' agreement regarding the Processing of Personal Data.

Customer enters into this DPA for itself and, if any of its Authorized Affiliates act as Controllers of Personal Data, on behalf of those Authorized Affiliates to the extent required under Data Protection Laws and Regulations. For the purposes of this DPA only, and except indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates (if applicable). All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer under the Agreement, Sitetracker may Process Personal Data on behalf of Customer. The parties agree to the following terms with respect to such Processing.

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Affiliate" means any Affiliate of Customer which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Sitetracker, but has not signed its own Order Form with Sitetracker and is not a "Customer" as defined in the Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer" means the entity that executed the Agreement, together with its Authorized Affiliates (for so long as they remain Affiliates), which have signed Order Form.

"Customer Data" means what is defined in the Agreement as "Customer Data", provided that such data is data and information provided by or for Customer to the Services.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**Data Subject Right**" means any right afforded to a Data Subject under Data Protection Laws and Regulations, including the rights to access, rectify, restrict the Processing of Personal Data, erasure (including the right to be forgotten), data portability, objecting to the Processing, or to not be subject to an automated individual decision making.

"GDPR" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to an identified or identifiable natural person, where such data is a part of Customer Data.

"Personal Data Breach" means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Sitetracker or its Sub-processors of which Sitetracker becomes aware.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or

destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Sitetracker" means Sitetracker Inc., a company incorporated in Delaware, U.S.A.

"Sitetracker Data Security Sheet" means Description of Sitetracker's Security Controls as set forth in the Schedule 3 of this DPA.

"Sitetracker Group" means Sitetracker and its Affiliates engaged in the Processing of Personal Data.

"Standard Contractual Clauses (UK)" or "UK SCCs" means the standard contractual clauses for the transfer of personal data pursuant to the European Commission's decision (C(2010)593) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**2021 Standard Contractual Clauses**" or "**2021 SCCs**" means the Annex to the European Commission's implementing decision (EU) 2021/914 (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union, and, where applicable, the Module II - "Controller to Processor" specified therein.

"**2021 Standard Contractual Clauses P2P**" or "**2021 SCCs P2P**" means the Module III - "Processor to Processor" of the 2021 Standard Contractual Clauses that Sitetracker may enter into with its Sub-processors.

"Sub-processor" means any Processor engaged by Sitetracker, by a member of the Sitetracker Group or by another Sub-processor in connection with its provision of Services.

"Supervisory Authority" means a governmental or government-chartered regulatory body having binding legal authority over Customer.

"Swiss Data Protection Laws" means Data Protection Laws and Regulations of Switzerland.

"UK Data Protection Laws" means Data Protection Laws and Regulations of the United Kingdom.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties agree that with regard to the Processing of Personal Data, Customer is the Controller, Sitetracker is the Processor, and applicable members of the Sitetracker Group will be engaged as Sub-processors in accordance with Section 5 ("SUB-PROCESSOR").

2.2. Customer Obligations Regarding Personal Data. In its use of the Services, Customer will comply with the Data Protection Laws and Regulations, including any applicable requirements to provide notice to and/or obtain consent from Data Subjects for Processing by Sitetracker. Customer shall ensure that its instructions for the Processing of Personal Data comply with Data Protection Laws and Regulations. Customer shall be solely responsible for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3. Sitetracker's Processing of Personal Data. Sitetracker shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Forms; (ii) Processing initiated by Customer personnel in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Sitetracker is prohibited from (i) selling the Personal Data or (ii) retaining, using, disclosing, or Processing Personal Data for any commercial or other purpose other than to perform the Services. Sitetracker will Process Personal Data in compliance with applicable Data Protection Laws and Regulations; provided, however, Sitetracker shall not be in violation of its contractual obligation herein in the event that Sitetracker's Processing of Personal Data in non-compliance with applicable Data Protection Laws and Regulations is due to Customer's misconducts.

2.4. Details of the Processing. The subject matter of the Processing of Personal Data by Sitetracker is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 of this DPA.

3. RIGHTS OF DATA SUBJECTS

Sitetracker shall, to the extent legally permitted and that Sitetracker has been able to identify the request comes from a Data Subject whose Personal Data was submitted to Sitetracker in connection with the Agreement by Customer, promptly notify

Customer if Sitetracker receives a request from a Data Subject in relation to the exercise of the Data Subject's Right (each such request being a "**Data Subject Request**"). To the extent legally permitted, Sitetracker will confirm to the Data Subject that it has passed the request to the Customer, but Sitetracker will not handle or execute the Data Subject Request. Without limiting the foregoing and taking into account the nature of the Processing, Sitetracker shall assist Customer by appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. Where such assistance exceeds the scope of requirements mandatorily imposed on the Processor by the applicable Data Protection Laws and Reguatlions , and to the extent legally permitted, Customer will be responsible for any additional, reasonable costs arising from the assistance.

4. SITETRACKER PERSONNEL

4.1. Confidentiality. Sitetracker shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.Sitetracker shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Limitation of Access. Sitetracker shall ensure that Sitetracker's access to Personal Data is limited to those personnel who require such access to perform the Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. Sitetracker's Affiliates may be retained as Sub-processors, and Sitetracker and its Affiliates may engage third-party Sub-processors in connection with the Services. Sitetracker or a Sitetracker Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data, to the extent applicable to the services provided by such Sub-processor.

5.2. Current Sub-processors and Notification of New Sub-processors. A list of Sub-processors for the Services, as of the date this DPA is executed, is attached in Schedule 1of this DPA. Sitetracker shall notify Customer in writing of any new Sub-processor before authorizing such new Sub-processor to Process Personal Data. The notification shall include an updated Sub-processor list which constitutes the information necessary to enable the Customer to exercise its right to object.

5.3. Objection Right for New Sub-processors. Customer may object to Sitetracker's use of a new Sub-processor by notifying Sitetracker in writing within five (5) business days after receipt of a notice described in Section 5.2 above. In the event Customer objects to a new Sub-processor, Sitetracker will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Sitetracker is unable to make available such change within a reasonable period of time, Customer may terminate the applicable portion of Order Form(s) with respect only to those affected Services which cannot be provided by Sitetracker without the use of the objected-to new Sub-processor, by promptly providing written notice in accordance with the "Notices" section of the Agreement.

5.4. Liability. Sitetracker shall be liable for the acts and omissions of its Sub-processors to the same extent Sitetracker would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1. Controls for the Protection of Customer Data. Sitetracker shall maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Customer Data (including protection against Personal Data Breach), in accordance with Sitetracker Data Security Sheet in Schedule 3 of this DPA. Sitetracker periodically monitors compliance with these measures. Customer is responsible for reviewing the information made available by Sitetracker relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws and Regulations. Customer acknowledges that the security measures described within the Sitetracker Data Security Sheet are subject to technical progress and development and that Sitetracker may update or modify such document from time to time, provided that such updates and modifications do not result in a material decrease of the overall security of the Services during the Term.

6.2. Third-Party Audit Reports and Certifications. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations in the Agreement, Sitetracker shall make available to Customer a copy of Sitetracker's then most recent SOC 2 audit report, and of any other audit reports and certifications that Sitetracker generally makes available to other customers, provided Customer is not a competitor of Sitetracker.

7. PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION

Sitetracker maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of a Personal Data Breach. Sitetracker shall provide information to Customer necessary to enable Customer to comply with its obligations under Data Protection Laws and Regulations in relation to such Personal Data Breach. Sitetracker shall make reasonable endeavor to identify the cause of such Personal Data Breach and take those steps as Sitetracker deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach to the extent the remediation is within Sitetracker's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or its personnel.

8. RETURN AND DELETION OF CUSTOMER DATA

At the termination or expiration of the Agreement, or upon Customer's reasonable request, Sitetracker and any Sub-processors will, at the choice of Customer, return all the Personal Data and copies of such data to Customer or securely destroy them. Upon receipt of Customer's reasonable requests, Sitetracker will demonstrate to the satisfaction of Customer that it has taken such measures. Notwithstanding the foregoing, in the event applicable laws or regulations prevent Sitetracker from returning or destroying all or part of the Personal Data, Sitetracker agrees to preserve the confidentiality of the Personal Data retained by it and that it will only actively Process such Personal Data after such date in order to comply with the applicable laws or regulations.

9. AUDIT

Upon Customer's request and at Customer's own cost, subject to the confidentiality obligations set forth in the Agreement, Sitetracker shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of Sitetracker and that has signed nondisclosure agreement reasonably acceptable to Sitetracker) information regarding the Sitetracker Group's compliance with the obligations set forth in this DPA in the form of Sitetracker's SOC 2 report and, for its Sub-processors, the third-party certifications and audit reports made available by them. Following any notice by Sitetracker to Customer of a Personal Data Breach, upon Customer's reasonable belief that Sitetracker is in breach of its obligations in respect of protection of Personal Data under this DPA, or if such audit is required by Customer's Supervisory Authority, Customer may contact Sitetracker in accordance with the "Notices" section of the Agreement to request an audit of the procedures relevant to the protection of Personal Data, provided that the written notice is provided at least thirty (30) days prior to such audit. Any such audit shall be conducted remotely, except Customer may conduct on-site audit at Sitetracker's premises during normal business hours if required by the Data Protection Laws and Regulations. Any such request shall occur no more than once annually, except in the event of an actual or reasonably suspected unauthorised access to Personal Data. Customer shall reimburse Sitetracker for any time expended for any such on-site audit at the Sitetracker Group's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any audit, Customer and Sitetracker shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Sitetracker. Customer shall promptly notify Sitetracker with information regarding any non-compliance discovered during the course of an audit. To the extent permitted under the applicable Data Protection Laws and Regulations, any audit of a Sub-processor shall be limited to a review of any reports, certifications and documentation made available by the Sub-processor, unless otherwise permitted with the Sub-processor's consent.

10. AUTHORIZED AFFILIATES

10.1. Contractual Relationship. By executing the Agreement, Customer enters into this DPA for itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Sitetracker and each such Authorized Affiliate subject to the provisions of the Agreement, this Section 10, and Section 11 ("LIMITATION OF LIABILITY"). Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement, and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

10.2. Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Sitetracker under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.3. Rights of Authorized Affiliates. Where an Authorized Affiliate is a party to this DPA, it may, to the extent required under applicable Data Protection Laws and Regulations, exercise its rights and seek remedies under this DPA, subject to the following:

10.3.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Sitetracker directly, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for

each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together.

10.3.2. The Customer entity that is the contracting party to the Agreement shall, when carrying out a permitted audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Sitetracker and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Sitetracker, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section, and such other sections that exclude or limit liability, of the Agreement, and any reference in such sections to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

12. EUROPE UNION AND SWITZERLAND SPECIFIC PROVISIONS

12.1. GDPR. Sitetracker will Process Personal Data in accordance with the GDPR requirements directly applicable to Sitetracker's provision of Services.

12.2. Transfer Mechanism for Data Transfers. As of the Effective Date of this DPA, with regard to any transfers of Personal Data under this DPA from the European Union or Switzerland to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations, Sitetracker makes available the following transfer mechanism(s) which shall apply, in the order of precedence as set out below:

12.2.1. Any valid transfer mechanism pursuant to applicable EU Data Protection Laws and Regulations (excluding the 2021 SCCs), to which Sitetracker would subscribe, certify or participate in, and for so long as such transfer mechanism is available and valid; or

12.2.2. The 2021 SCCs, when they are an available and a valid transfer mechanism under applicable Data Protection Laws and Regulations, and the parties acknowledge and agree that they will comply with the 2021 SCCs provisions as set out below:

a) **General.** When entering into the 2021 SCCs, Customer and any applicable Authorized Affiliates are each the data exporter, and Sitetracker are the data importer. The additional terms in this Section 12.2.2 below also apply to such data transfers.

b) **Customers Covered by the 2021 SCCs.** The 2021 SCCs and the additional terms specified in this Section 12.2.2 apply to (i) Customer, to the extent Customer is subject to the applicable Data Protection Laws and Regulations of the European Union and/or their Member States, or Switzerland, and (ii) its Authorized Affiliates (if applicable).

c) **2021 SCCs Clause 7 - Docking clause.** The option under clause 7 shall not apply.

d) **2021 SCCs Clause 8.1 - Instructions.** The following are deemed to be instructions by the Customer to process Personal Data: (a) the Agreement, applicable schedules attached thereto, and applicable Order Forms, and (b) commands and actions initiated by Customer users in their use of the Services. For clarification, the instructions by Customer to Process Personal Data include onward transfers to a third party located outside the applicable Member State, or Switzerland, for the purpose of the performance of the Services.

e) **2021 SCCs Clause 8.3 - SCCs Copy**. On request by a Data Subject, the Customer may make a copy of the 2021 SCCs, available to the Data Subject in accordance with Clause 8.3. Customer shall not make the entirety of this DPA available, but a copy of the 2021 SCCs (including the relevant Schedules of this DPA) only. Customer shall make commercially reasonable efforts to consult Sitetracker in order to redact the 2021 SCCs and/or the relevant Schedules of this DPA to the extent necessary to protect Sitetracker's Confidential Information, prior to sharing them with the Data Subject, and shall not disclose any of Sitetracker's Confidential Information without Sitetracker's written consent. The parties shall make good faith efforts to coordinate the response to the Data Subject regarding the reasons for the redactions, to the extent possible without revealing the redacted information.

f) **2021 SCCs Clause 8.4 - Accuracy.** Sitetracker will provide reasonable assistance to Customer to erase or rectify inaccurate Personal Data in accordance with Clause 8.4, by providing appropriate technical and organizational measures, where possible through the Services and/or as outlined in applicable Documentation.

g) **2021 SCCs Clause 8.5 and 16(b) - Certification of Deletion.** The parties agree that the certification of deletion of Personal

Data that is described in clause 8.5 and 16(d) shall be provided by Sitetracker to Customer only upon Customer's written request.

h) **2021 SCCs Clause 8.6 - Security of Processing**. The parties agree that Sitetracker shall comply with its obligations under Clause 8.6(d) by providing assistance to the Customer in the event of a Personal Data Breach in accordance with Section 7 ("PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION"). Sitetracker conducts regular checks of the technical and organisational measures required by Clause 8.6 in the form of audit reports and certification.

i) **2021 SCCs Clause 8.9 - Audit Rights.** Audits pursuant to Clause 8.9 of the 2021 SCCs shall be carried out in accordance with Section 9 ("AUDIT").

j) **2021 SCCs Clause 9 - Sub-processors.** Section 5 ("SUB-PROCESSOR") and Schedule 1 of this DPA represents Customer's general authorization for the engagement of existing and new Sub-processors under Clause 9(a) of the 2021 SCCs. The parties agree that data transfers to Sub-processors may rely on an available transfer mechanism under applicable Data Protection Laws and Regulations other than the 2021 SCCs (for example, binding corporate rules), and that Sitetracker's agreements with such Sub-processors may therefore not incorporate or mirror the 2021 SCCs. Sitetracker shall only on request by Customer, pursuant to Clause 9(c) of the 2021 SCCs, make a copy of the Sub-processor agreements, including applicable 2021 SCCs P2P, available to Customer. To the extent necessary to protect business secrets other Confidential Information, Sitetracker and the Sub-processor may have all commercial information, or clauses unrelated to the 2021 SCCs P2P, removed by Sitetracker beforehand. Sitetracker shall in accordance with Clause 9(d) notify the Customer of any failure by the Sub-processor to fulfil its obligations under the 2021 SCCs P2P where such a failure amounts to a breach of the 2021 SCCs P2P that leads to Sitetracker being in material breach of this DPA. Any and all communications, instructions, notifications, enquiries, requests, correspondence, co-operation, and assistance between Customer and Sub-processors, provided by the 2021 SCCs or 2021 SCCs P2P, shall be made exclusively via Sitetracker.

k) **2021 SCCs Clause 12 - Liability.** Sitetracker's liability under clause 12(b) shall be limited to any damage caused by its Processing where Sitetracker has not complied with its obligations under the GDPR, or other applicable Data Protection Laws and Regulations, specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR or the equivalent provisions of applicable Data Protection Laws and Regulations.

l) **2021 SCCs Clause 14 - Transfer Impact Assessments.** Upon Customer request, Sitetracker will make available to Customer its documented assessment of its processing of Personal Data hereunder for the purpose of Clause 14 and the parties agree that such assessment provides to Customer the relevant information that a data importer is required to provide to a data exporter in accordance with clause 14 (b) and clause 14 (c).

m) **2021 SCCs Clauses 14 (f), 16 (b) and 16 (c) - Suspension and Termination.** Where Customer exercises any of its rights to suspend the processing of Personal Data within the Services or its right to terminate any applicable Order Form(s) pursuant to Clauses 14 (f), 16 (b) or16 (c):

i. Customer shall notify Sitetracker in writing setting forth in reasonable detail the alleged or actual material non-compliance with the requirements of the 2021 SCCs ("**Compliance Situation**") and shall provide the factual basis for such determination and identify the provisions of the 2021 SCCs with which, in the Customer's reasonable opinion, there is a material non-compliance by Sitetracker and the applicable Data Protection Laws and Regulations that are not met; and

ii. without prejudice to any other rights or remedies available to either party under this DPA, the Agreement, or otherwise, if Customer cannot implement a commercially reasonable change to its configuration or use of the Services to avoid such Compliance Situation, and if within sixty (60) days after receipt of such notice by Sitetracker or any other timeframe agreed by the parties, Sitetracker does not: (1) demonstrate that the Compliance Situation does not lead to a violation of the 2021 SCCs, (2) make available to Customer a change in the Services that remedies such Compliance Situation without unreasonably burdening Customer, or (3) recommend a commercially reasonable change in Customer's use or configuration of the Services that remedies such Compliance Situation without unreasonably burdening Customer; then

iii. Customer may terminate the applicable portion of Order Form(s) with respect only to those affected Services which cannot be provided by Sitetracker pursuant to the 2021 SCCs, by promptly providing written notice in accordance with the "Notices" section of the Agreement.

n) **2021 SCCs Clause 15.1 (a) - Data Subject Notification.** To the extent legally permitted, any and all communications, instructions, notifications, enquiries, requests, correspondence, co-operation, and assistance needs between Sitetracker and Data Subjects intended under the 2021 SCCs shall be made exclusively via Customer.

o) **2021 SCCs Clause 15.1 (a) - Notification of Government Access Requests.** For the purposes of clause 15(1)(a), Sitetracker shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject.

p) **2021 SCCs Clause 15.1 (c) - Information Regarding Received Requests.** To the extent legally permitted, Sitetracker shall

make information regarding received requests available to Customer only upon Customer's reasonable written requests.

q) **2021 SCCs Clause 17 - Governing Law.** The parties agree, with respect to OPTION 2 to Clause 17, that in the event that the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, the SCCs shall be governed by the law of Ireland.

r) **2021 SCCs Clause 18 - Choice of Forum and Jurisdiction.** In accordance with Clause 18, disputes associated with the 2021 SCCs shall be resolved by the courts specified in the Agreement, unless such court is not located in an EU Member State, in which case the forum for such disputes shall be the courts of Ireland.

s) **Annexes.** For purposes of execution of 2021 SCCs, Schedule 2: Details of the Processing shall be incorporated as ANNEX I, Schedule 3: Sitetracker Security Controls shall be incorporated as ANNEX II, and Schedule 1: Current Sub-Processor List shall be incorporated as ANNEX III.

t) **Interpretation.** The terms of this DPA are intended to clarify and not to modify the 2021 SCCs. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules and the 2021 SCCs, the 2021 SCCs shall prevail.

12.2.3. Data Exports from Switzerland under the 2021 SCCs. If any transfers of Personal Data from Switzerland exclusively subject to the Swiss Data Protection Laws, (i) general and specific references in the 2021 SCCs to GDPR or EU Member State Law shall have the same meaning as the equivalent reference in the Swiss Data Protection Laws, (ii) references in the 2021 SCCs to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of Switzerland", and (iii) any other obligation in the 2021 SCCs determined by the Member State in which the data exporter or Data Subject is established shall refer to an equivalent obligation under Swiss Data Protection Laws.

13. <u>UNITED KINGDOM SPECIFIC PROVISIONS</u>

13.1 UK Data Protection Laws. Sitetracker will Process Personal Data in accordance with the requirements of UK Data Protection Laws directly applicable to Sitetracker's provision of its Services.

13.2 Transfer Mechanism for Data Transfers. As of the Effective Date of this DPA, the UK SCCs apply to any transfers of Personal Data under this DPA from the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of UK Data Protection Laws, to the extent such transfers are subject to UK Data Protection Laws. When entering into the UK SCCs, Customer and any applicable Authorized Affiliates are each the data exporter, and Sitetracker are the data importer. Parties agree that (i) general and specific references in the UK SCCs to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 shall hereby be deemed to have the same meaning as the equivalent reference in the UK Data Protection Laws; (ii) references in the UK SCCs to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of the United Kingdom"; and (iii) any other obligation in the UK SCCs determined by the Member State in which the data exporter is established shall hereby be deemed to refer to an equivalent obligation under UK Data Protection Laws. The additional terms in the Section 13.3 below also apply to such data transfers.

13.3Additional Terms for Transfers Subject to the Standard Contractual Clauses (UK).

13.3.1 Customers Covered by the UK SCCs. The UK SCCs and the additional terms specified in this Section 13.3 apply to (i) Customer, to the extent Customer is subject to UK Data Protection Laws and, (ii) its Authorized Affiliates (if applicable).

13.3.2 Instructions. For the purposes of Clause 5(a) of the UK SCCs, the following are deemed to be instructions by the Customer to process Personal Data: (a) the Agreement, applicable schedules attached thereto, and Order Forms, and (b) commands and actions initiated by Customer users in their use of the Services. For clarification, the instructions by Customer to Process Personal Data include onward transfers to a third party located outside United Kingdom for the purpose of the performance of the Services.

13.3.3 New Sub-processors. Section 5 ("SUB-PROCESSORS") and Schedule 1 of this DPA represents Customer's general authorization for the engagement of existing and new Sub-processors under Clause 5(h) of the UK SCCs. Pursuant to Clause 5(h) of the UK SCCs, Customer agrees that Sitetracker may engage new Sub-processors as described in Section 5. The parties agree that data transfers to Sub-processors may rely on an available transfer mechanism other than the UK SCCs (for example, binding corporate rules), and that Sitetracker's agreements with such Sub-processors may therefore not incorporate or mirror the UK SCCs. The parties further agree that to the extent necessary to protect business secrets, personal data or other Confidential Information, the copies of the Sub-processor agreements that must be provided by Sitetracker to Customer pursuant to Clause 5(j) of the UK SCCs may have all commercial information, or clauses unrelated to the UK SCCs or their equivalent, removed by Sitetracker beforehand; and, that such copies will be provided by Sitetracker only upon the written request of Customer.

13.3.4 Audits and Certifications. The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the UK

SCCs shall be carried out in accordance with Section 9 (“AUDIT”).

13.3.5 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the UK SCCs shall be provided by Sitetracker only upon Customer’s request.

13.3.6 Appendices. For purposes of execution of the UK SCCs, Schedule 2: Details of the Processing shall be incorporated as Appendix 1, and Schedule 3: Sitetracker Security Controls shall be incorporated as Appendix 2.

13.3.7 Interpretation. The terms of this DPA are intended to clarify and not to modify the UK SCCs. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules and the UK SCCs, the UK SCCs shall prevail.

14. **DATA PROTECITON IMPACT ASSESSMENT**

Upon Customer’s request, Sitetracker shall reasonably cooperate with and assist Customer in fulfilling Customer’s obligations under applicable Data Protection Laws and Regulations/UK Data Protection Laws to carry out a data protection impact assessment related to Customer’s use of the Services, to the extent Customer does not otherwise have access to the relevant information and such information is available to Sitetracker. Sitetracker shall reasonably assist Customer in its cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 14, to the extent required under applicable Data Protection Laws and Regulations/UK Data Protection Laws.

The parties' authorized signatories have duly executed this DPA:

SITETRACKER, INC.	**CUSTOMER**
By:	By:
Name: Giuseppe Incitti	Name:
Title: Chief Executive Officer	Title:
Date:	Date:

LIST OF SCHEDULES

Schedule 1: Current Sub-processor List

Schedule 2: Details of the Processing

Schedule 3: Description of Sitetracker's Security Controls

SCHEDULE 1

Current Sub-processor List

(effective as of the Effective Date; subject to change)

Sitetracker uses certain Sub-processors, whether third parties or subsidiaries of Sitetracker (as described below), who process Personal Data on behalf of Sitetracker and in connection with Sitetracker's provision of the Services to its customers.

What follows is the list of current Sub-processors that Sitetracker uses in its provision of the Services. Depending upon a Customer's use of the Services, e.g. geographical location of the Customer, not all listed Sub-Processors will be needed to deliver the Services. Sub-processors receive, store, structure, categorize, analyze, handle, process and send Personal Data, as applicable and only to the extent necessary for the provision of the Services in accordance with this DPA and the Agreement. The Sub-processors Process Personal Data until the earlier of (i) the completion of the Processing provided by such Sub-processor, or (ii) the duration of the Agreement, subject to the terms of the Agreement, schedules attached thereto, this DPA, and the applicable documentation.

Customers shall provide appropriate contact details to Sitetracker in order to receive notice of new Sub-processors.

Infrastructure Sub-processor

Sitetracker may use the following Sub-processor to host Customer Data or provide other infrastructure that helps with the delivery of Services:

Entity Name	Sub-processing Activities	Entity Country	Processing Country
Salesforce, Inc.	Cloud Service Provider	United States	EU, EEA

Other Sub-processors

Sitetracker may use the following Sub-processors to perform other Services-related functions:

Entity Name	Sub-processing Activities	Entity Country	Processing Country
Twilio, Inc.	Cloud-Based Email Delivery and SMS Notification Services	United States	United States
Google LLC	Email and Document Storage	United States	United States
PagerDuty, Inc.	Incident Response Services	United States	United States
ProductBoard, Inc.	Customer Feedback Repository	United States	United States
Thought Industries, Inc.	Customer Certifications, Training, and Help Documentation	United States	United States
Stripe, Inc.	*Optional - Cloud-Based Payment Processing Services*	United States	United States

Sitetracker Affiliates

Depending on the geographic location of the Customer or their Authorized Users, and the nature of the Services provided, Sitetracker may also engage its affiliate, Sitetracker UK Limited, Sitetracker Luxembourg S.a.r.l, Sitetracker Germany GmbH, and(or) Sitetracker Spain, S.L. to deliver some or all of the Services provided to a Customer.

SCHEDULE 2

Details of the Processing

Nature and Purpose of Processing

Sitetracker will Process Personal Data as necessary to perform the Services pursuant to the Agreement and Order Forms, as further specified in applicable SOW and Documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Section 8 of this DPA ("RETURN AND DELETION OF CUSTOMER DATA"), Sitetracker will Process Personal Data for the duration of the Agreement, Order Forms, and SOWs (as applicable), unless otherwise agreed in writing.

Frequency of the Transfer

Subject to specified duration of Processing in the foregoing, Personal Data is transferred on a continuous basis so long as it is necessary for the provision of Services.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's users authorized by data exporter to use the Services

Types of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (email, phone, physical business address, etc.)
- Localisation data (including device data)

Special Categories of Data

Not applicable.

Sub-processing Description

Subject matter, nature, and duration provided under the preamble of the Schedule 1 of this DPA.

Competent Supervisory Authority

The Data Protection Commission of Ireland

SCHEDULE 3

Description of Sitetracker's Security Controls

(*effective as of October 2021; subject to change without notice*)

Introduction

The goal of this document is to provide high-level information to our customers regarding Sitetracker's commitment to security and data protection.

1. Annual Evidence of Compliance

(a) Third Party Security Audit

Sitetracker shall continue to be annually audited against the SOC 2 Type II standard, at Sitetracker's expense. Although that report provides an independently-audited confirmation of Sitetracker security posture annually, the most common points of interest are further detailed below.

(b) Executive Summary of Web Application Penetration Test

Sitetracker shall continue to annually engage an independent, third-party to perform a web application penetration test. The third party web application penetration test shall be done at least annually and vulnerabilities as defined by industry standards shall be remediated within a reasonable risk based timeframe, or identified as a residual risk where action(s) should be taken to remediate as soon as possible.

(c) Security Awareness Training

Sitetracker shall provide annual Security Awareness training to all personnel. Security Awareness training shall address security topics to educate users about the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms. Training materials should address industry standard topics which include, but are not limited to:

- The importance of information security, the consequences of information security failures and how to report a security breach.
- Physical controls such as visitor protocols, safeguarding portable devices and proper data destruction.
- Logical controls related to strong password selection/best practices.
- How to recognize social engineering attacks such as phishing.

(d) Vulnerability Scan

Sitetracker shall ensure that vulnerability scans are completed at minimum annually using an industry standard vulnerability scanning tool. All cloud hosted systems shall be scanned, where applicable and where approved by cloud service provider.

2. General Controls. Sitetracker shall implement, or be responsible for its Sub-processor's implementation of, measures designed to:

(a) deny unauthorised persons access to data-processing equipment used for processing Personal Data (equipment access control);

(b) prevent the unauthorised reading, copying, modification or removal of data media containing Personal Data (data media control);

(c) prevent the unauthorised inspection, modification or deletion of stored Personal Data (storage control);

(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment used to process Personal Data (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the Personal Data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which individuals Personal Data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which Personal Data have been put into automated data-processing systems and when and by whom the input was made (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of Personal Data during transfers of those data or

during transportation of data media (transport control);

(i) ensure that installed systems used to process Personal Data may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system used to process Personal Data perform, that the appearance of faults in the functions is reported (reliability) and to prevent stored Personal Data from corruption by means of a malfunctioning of the system (integrity).

3. **Personnel.** Sitetracker shall take reasonable steps to ensure that no person shall be appointed by Sitetracker to process Personal Data unless that person:

(a) is competent and qualified to perform the specific tasks assigned by Sitetracker;

(b) has been authorised by Sitetracker; and

(c) has been instructed by Sitetracker in the requirements relevant to the performance of the obligations of Sitetracker under these Clauses, in particular the limited purpose of the data processing.

4. **Copy Control.** Sitetracker shall not make copies of Personal Data, provided, however, Sitetracker may retain copies of Personal Data provided to it for backup and archive purposes, under the terms set forth in the Agreement and this DPA.

5. **Security Controls.** The Services include a variety of configurable security controls that allow the Customer to tailor the security of the Services for its own use. These controls include:

- Unique User identifiers (User IDs) to ensure that activities can be attributed to the responsible individual.
- Controls to revoke access after several consecutive failed login attempts.
- The ability to specify the lockout time period.
- Controls on the number of invalid login requests before locking out a User.
- Controls to ensure generated initial passwords must be reset on first use.
- Controls to force a User password to expire after a period of use.
- Controls to terminate a User session after a period of inactivity.
- Password history controls to limit password reuse.
- Password length controls.
- Password complexity requirements (requires letters and numbers, and special characters).
- Verification question before resetting password.
- The ability to accept logins to the Services from only certain IP address ranges.
- The ability to restrict logins to the Services to specific time periods.
- Ability to delegate user authentication or federate authentication via SAML.

6. **Security Procedures, Policies and Logging.** The Services are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a one-way hashing algorithm (SHA-256) and are never transmitted unencrypted.
- User access log entries will be maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If there is suspicion of inappropriate access, Sitetracker or its Sub-processor can provide Customer log entry records to assist in forensic analysis. This service will be provided to Customer on a time and materials basis.
- Logging will be kept for a minimum of 90 days.
- Logging will be kept in a secure area to prevent tampering.
- Passwords are not logged under any circumstances.
- Certain administrative changes to the Services (such as password changes and adding custom fields) are tracked in an area known as the "Setup Audit Log" and are available for viewing by Customer's system administrator. Customer may download and store this data locally.
- Processor's personnel will not set a defined password for a User. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting User.

7. **Intrusion Detection.** Sitetracker, or an authorised third party (subject to the terms of these Clauses), will monitor the Services for unauthorised intrusions using network-based intrusion detection mechanisms.

8. **User Authentication.** Access to the Services requires a valid User ID and password combination, which are encrypted via TLSv1.2 while in transmission. Following a successful authentication, a random session ID is generated and stored in the user's

browser to preserve and track session state.

9. **Security Logs.** Sitetracker shall ensure that all Sitetracker or Sub-processor systems used to store Customer Data, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralised syslog server (for network systems).

10. **Incident Management.** Sitetracker maintains security incident management policies and procedures.

11. **Physical Security.** Sitetracker Sub-processor's production data centres have an access system that controls access to the data centre. This system permits only authorised personnel to have access to secure areas. The facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, biometric access screening and escort-controlled access, and is also supported by on- site back-up generators in the event of a power failure.

12. **Reliability and Backup.** All networking components, SSL accelerators, load balancers, Web servers and application servers that are part of the Force.com platform are configured in a redundant configuration. All Personal Data is stored on a primary database server that is clustered with a backup database server for redundancy. All Personal Data is stored on carrier-class disk storage using RAID disks and multiple data paths. All Personal Data, up to the last committed transaction, is automatically backed up on a regular basis. Any backup tapes are verified for integrity stored in an off-site facility in a secure, fire-resistant location.

13. **Disaster Recovery.** Sitetracker will ensure that the systems where Customer's Personal Data is stored have a disaster recovery facility that is geographically remote from its primary data centre, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centre were to be rendered unavailable.

14. **Viruses.** The Services will not introduce any viruses to Customer's systems; however, the Services do not scan for viruses that could be included in attachments or other Personal Data uploaded into the Services by Customer. Any such uploaded attachments will not be executed in the Services and therefore will not damage or compromise the Service.

15. **Data Encryption.** The Services use industry-accepted encryption products to protect Customer's Personal Data and communications during transmissions between a customer's network and the Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, Customer's Personal Data is encrypted during transmission between data centres for replication purposes. The Services permit the encryption at rest with 256-bit master keys and use the Advanced Encryption Standard (AES) algorithm of custom fields.

16. **System Changes and Enhancements.** Sitetracker plans to enhance and maintain the Services during the term of the Agreement. Security controls, procedures, policies and features may change or be added. Sitetracker will provide security controls that deliver a level of security protection that is not materially lower than that provided as of the Effective Date, informing the Customer with due notice in relation to any changes to be implemented regarding the measures referred to herein.