Data Processing Addendum

This Data Processing Addendum ("**DPA**"), including its Attachments and Appendices, forms part of the subscription agreement, Algolia's Terms of Service available at https://algolia.com/policies/terms or other written or electronic agreement (the "**Agreement**"), including any written or electronic service orders, purchase orders or other order forms (each a "**Service Order**") entered into between Algolia and Subscriber, pursuant to which Algolia provides the "**Services"** as defined in the Agreement.

The purpose of this DPA is to reflect the parties' agreement with regard to the processing of Subscriber Personal Data. The parties agree to comply with this DPA with respect to any Subscriber Personal Data that the Algolia Group may process in the course of providing the Services pursuant to the Agreement. This DPA shall not replace or supersede any data processing addendum or agreement executed by the parties prior to the DPA Effective Date without the prior written consent of the parties (electronically submitted consent acceptable).

This DPA will take effect on the DPA Effective Date and, notwithstanding expiry of the Term, will remain in effect until, and automatically expire upon, deletion of all Subscriber Data by Algolia as described in this DPA.

If the Subscriber entity entering into or accepting this DPA is neither a party to a Service Order nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Subscriber entity that is a party to the Agreement executes this DPA.

For the purposes of this DPA, the Algolia entity entering into this DPA as the data processor shall depend on the location of the Subscriber. For Subscribers in Europe, the Algolia contracting entity to this DPA is Algolia SAS. For Subscribers outside of Europe, the Algolia contracting entity to this DPA is Algolia, Inc.

By signing or accepting the Agreement or this DPA, Subscriber enters into this DPA as of the DPA Effective Date on behalf of itself and in the name and on behalf of its Covered Affiliates if and to the extent the Algolia Group processes personal data for which such Covered Affiliates qualify as the controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Subscriber" shall include Subscriber and its Covered Affiliates.

1. Definitions

1.1. Capitalized terms used but not defined in this DPA shall have the meaning given to them in the Agreement or applicable Data Protection Laws.

"**Affiliates**" of a party is any entity (a) that the party Controls; (b) that the party is Controlled by; or (c) with which the party is under common Control, where "**Control**" means direct or indirect control of fifty percent (50%) or more of an entity's voting interests (including by ownership).

"**Algolia**" means either (i) Algolia, Inc., a company incorporated in Delaware, with offices at 301 Howard St, 3rd floor, San Francisco, CA 94105, if Subscriber is domiciled in a country located outside of Europe or (ii) Algolia SAS, a French société par actions simplifiées, with offices at 55 Rue d'Amsterdam, 75008 Paris, France, if Subscriber is domiciled in a country in Europe.

"**Algolia Group**" means Algolia and its Affiliates engaged in the processing of Subscriber Personal Data in connection with the subscribed Services.

"**Covered Affiliate**" means any of Subscriber's Affiliate(s) which (a) is subject to the Data Protection Laws; and (b) is permitted to use the Services pursuant to the Agreement between Subscriber and Algolia, but has not signed its own Service Order with Algolia and is not a "Subscriber" as defined under the Agreement.

"Data Incidents" means a breach of Algolia's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Subscriber Data transmitted, stored or otherwise processed by Algolia. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Subscriber Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Data Protection Laws" means all applicable data protection and privacy laws and regulations, including EU/UK Data Protection Laws.

"**DPA Effective Date**" means, as applicable, (a) September 27, 2021 if Subscriber clicked to accept or the parties otherwise agreed to this DPA prior to or on such date; or (b) the date on which Subscriber clicked to accept or the parties otherwise agreed to this DPA, if such date is after September 27, 2021.

"**EEA**" means the European Economic Area.

"**EU/UK Data Protection Laws**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

"**Restricted Transfer**" means (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Security Documentation**" means all documents and information made available by Algolia to demonstrate compliance by Algolia with its obligations under this DPA, including the Security Measures, Additional Security Information and any third-party certifications or audit reports, as applicable.

"**Security Measures**" means the technical and organizational safeguards adopted by Algolia applicable to the Services subscribed by Subscriber as described and made available at https://www.algolia.com/security/measures or as otherwise made available by Algolia. The Security Measures as of September 27, 2021 are attached to this DPA as Attachment 2.

"Standard Contractual Clauses" (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

"**Sub-processor**" means any third-party engaged by Algolia, including any member of the Algolia Group which processes Subscriber Data in order to provide parts of the Services as listed on https://www.algolia.com/policies/infrastructure-and-sub-processors/. Where (i) Subscriber is domiciled in a country located outside Europe, Algolia, Inc. acts as the data processor and other Affiliates of the Algolia Group act as Sub-processors, and where (ii) Subscriber is domiciled in a country inside Europe, Algolia SAS acts as the data processor and other Affiliates of the Algolia Group act as Sub-processors.

"**Subscriber**" means the subscriber entity party to the Agreement. Subscriber may also be referred to as "**Customer**" in the Agreement from time to time.

"**Subscriber Data**" has the meaning given to it in the Agreement or, if no such meaning is given, means

data submitted by or on behalf of Subscriber to the Services under the Subscriber's Algolia account for Services. Subscriber Data may also be referred to as "**Customer Data**" in the Agreement from time to time.

"**Subscriber Personal Data**" means the personal data contained within Subscriber Data. Subscriber Personal Data may also be referred to as "**Customer Personal Data**" in the Agreement from time to time.

"**Term**" means the period from the DPA Effective Date until the end of Algolia's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Algolia may continue providing the Services for transitional purposes.

1.2. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this DPA have the meanings given in the EU/UK Data Protection Laws, and the terms "data importer" and "data exporter" have the meanings given in the Standard Contractual Clauses, in each case irrespective of whether other Data Protection Laws apply.

2. Personal Data Processing Terms

2.1. The parties agree that if the EU/UK Data Protection Laws apply to the processing of Subscriber Personal Data, the parties acknowledge and agree that:

2.1.1. With respect to Subscriber Personal Data, Subscriber is the controller (or, where Subscriber is instructing Algolia on behalf of a third party controller, a processor on behalf of that controller) and Algolia is either (i) the processor or, (ii) where Subscriber is a processor on behalf of a third party controller, Algolia shall be a sub-processor to Subscriber.

2.1.2. Algolia may engage Sub-processors pursuant to Section 7 (Sub-processors).

2.1.3. The subject-matter of the data processing covered by this DPA is the provision of the Services and the processing will be carried out for the duration of the Agreement or so long as Algolia is providing the Services. Attachment 1 of this DPA sets out the nature and purpose of the processing, the types of Subscriber Personal Data Algolia processes and the categories of data subjects whose Personal Data is processed.

2.1.4. Each party will comply with the obligations applicable to it under the EU/UK Data Protection Laws, including with respect to the processing of Subscriber Personal Data.

2.1.5. If Subscriber is a processor itself, Subscriber warrants to Algolia that Subscriber's instructions and actions with respect to the Subscriber Personal Data, including its appointment of Algolia as a sub-processor, have been authorized by the relevant controller.

2.1.6. For the avoidance of doubt, Subscriber's instructions to Algolia for the processing of Subscriber Personal Data shall comply with all applicable laws, including the EU/UK Data Protection Laws. As between Algolia and Subscriber, Subscriber shall be responsible for the Subscriber Data and the means by which Subscriber acquired Subscriber Data, and shall maintain such authorizations and all other approvals, consents and registrations as are required to carry out lawful personal data processing activities under Data Protection Laws.

2.1.7. For the purposes of this DPA, the following is deemed an instruction by Subscriber to process Subscriber Personal Data (a) to provide the Services; (b) as further specified via Subscriber's use of the Services (including the Services' user interface dashboard and other functionality of the Services); (c) as documented in the Agreement (including this DPA and any Service Order that requires processing of Subscriber Personal Data); and (d) as further documented in any other written instructions given by Subscriber (which may be specific instructions or instructions of a general nature as set out in this DPA, the Agreement or as otherwise notified by Subscriber to Algolia from time to time), where such instructions are consistent with the terms of the Agreement.

2.1.8. When Algolia processes Subscriber Personal Data in the course of providing the Services, Algolia will:

2.1.8.1. Process the Subscriber Personal Data only in accordance with (a) the Agreement and (b) Subscriber's instructions as described in Section 2.1.7, unless Algolia is required to process Subscriber Personal Data for any other purpose by UK, European Union or member state law to which Algolia is subject. Algolia shall inform Subscriber of this requirement before processing unless prohibited by applicable laws on important grounds of public interest.

2.1.8.2. Notify Subscriber without undue delay if, in Algolia's opinion, an instruction for the processing of Subscriber Personal Data given by Subscriber infringes applicable EU/UK Data Protection Laws.

2.2. The parties acknowledge and agree that the parties will comply with all applicable laws with respect to the processing of Subscriber Personal Data.

3. Data Security

3.1. Security Measures

3.1.1. Algolia will implement and maintain appropriate technical and organizational measures designed to protect or secure (i) Subscriber Data, including Subscriber Personal Data, against unauthorized or unlawful processing and against accidental or unlawful loss, destruction or alteration or damage, unauthorized disclosure of, or access to, Subscriber Data, and (ii) the confidentiality and integrity of Subscriber Data, as set forth in the Security Measures. Algolia may update or modify the Security Measures from time to time provided that such updates and modifications will not materially decrease the overall security of the Services. The most up to date Security Measures will be made available at https://www.algolia.com/security/measures.

3.1.2. In addition to the Security Measures, Algolia will, from time to time, make additional security guidelines available that provide Subscriber with information about, in Algolia's opinion, best practices for securing, accessing and using Subscriber Data including best practices for password and credentials protection ("**Additional Security Information**").

3.1.3. Algolia will take reasonable steps to ensure the reliability and competence of Algolia personnel engaged in the processing of Subscriber Personal Data.

3.1.4. Algolia will take appropriate steps to ensure that all Algolia personnel engaged in the processing of Subscriber Personal Data (i) comply with the Security Measures to the extent applicable to their scope of performance, (ii) are informed of the confidential nature of the Subscriber Personal Data, (iii) have received appropriate training on their responsibilities, and (iv) have executed written confidentiality agreements. Algolia shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

3.2. Data Incidents

3.2.1. If Algolia becomes aware of a Data Incident, Algolia will: (a) notify Subscriber of the Data Incident without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Subscriber Data.

3.2.2. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and, as applicable, steps Algolia recommends Subscriber to take to address the Data Incident.

3.2.3. Notification(s) of any Data Incident(s) will be delivered to Subscriber in accordance with the "Manner of Giving Notices" Section of the Agreement or, at Algolia's discretion, by direct communication (for example, by phone call or an in-person meeting). Subscriber is solely

responsible for ensuring that any contact information, including notification email address, provided to Algolia is current and valid.

3.2.4. Algolia will not assess the contents of Subscriber Data in order to identify information subject to any specific legal requirements. Subscriber is solely responsible for complying with incident notification laws applicable to Subscriber and fulfilling any third-party notification obligations related to any Data Incident(s).

3.2.5. Algolia's notification of or response to a Data Incident under this Section 3.2 (Data Incidents) will not be construed as an acknowledgement by Algolia of any fault or liability with respect to the Data Incident.

3.3. Subscriber's Security Responsibilities and Assessment of Algolia

3.3.1. Subscriber agrees that, without prejudice to Algolia's obligations under Section 3.1 (Security Measures) and Section 3.2 (Data Incidents):

3.3.1.1. Subscriber is solely responsible for its use of the Services, including: (i) making appropriate use of the Services and any Additional Security Information to ensure a level of security appropriate to the risk in respect of the Subscriber Data; (ii) securing the account authentication credentials, systems and devices Subscriber uses to access the Services; and (iii) backing up the Subscriber Data; and

3.3.1.2. Algolia has no obligation to protect Subscriber Data that Subscriber elects to store or transfer outside of Algolia's and its Sub-processors' systems (for example, offline or on-premises storage).

3.3.2. Subscriber is solely responsible for reviewing the Security Measures and evaluating for itself whether the Services, the Security Measures, the Additional Security Information and Algolia's commitments under this Section 3 (Data Security) will meet Subscriber's needs, including with respect to any security obligations of Subscriber under the Data Protection Laws. Subscriber acknowledges and agrees that the Security Measures implemented and maintained by Algolia as set out in Section 3.1 (Security Measures) provide a level of security appropriate to the risk in respect of the Subscriber Data.

3.4. Subscriber Assessment and Audit of Algolia Compliance

Upon Subscriber's written request, at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Algolia will make available to Subscriber that is not a competitor of Algolia (or Subscriber's independent, third-party auditor that is not a competitor of Algolia) information regarding Algolia's compliance with the obligations set forth in this DPA including in the form of independent audit results and/or third-party certifications, as applicable, to the extent Algolia makes them generally available to its subscribers. The most recent independent third-party certifications or audits obtained by Algolia are set forth in the Security Measures.

3.5. Subscriber's Audit Rights

3.5.1. No more than once per year, Subscriber may contact Algolia in accordance with the "Manner of Giving Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Subscriber Data. Subscriber shall reimburse Algolia for any time expended for any such on-site audit. Before the commencement of any such on-site audit, Subscriber and Algolia shall mutually agree upon the scope, timing, and duration of the audit, that reasonably does not interfere with normal business operations, in addition to the reimbursement rate for which Subscriber shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Algolia. Subscriber shall promptly notify Algolia with information regarding any non- compliance discovered during the course of an audit.

3.5.2. Subscriber may conduct such on-site audit (a) itself, (b) through an Affiliate that is not a competitor of Algolia or (c) through an independent, third-party auditor that is not a competitor of Algolia.

3.5.3. Subscriber may also conduct an audit to verify Algolia's compliance with its obligations under this DPA by reviewing the Security Documentation.

4. Return or Deletion of Subscriber Data

4.1. Algolia will enable Subscriber to delete during the Term Subscriber Data in a manner consistent with the functionality of the Services. If Subscriber uses the Services to delete any Subscriber Data during the Term and that Subscriber Data cannot be recovered by Subscriber, this use will constitute an instruction to Algolia to delete the relevant Subscriber Data from Algolia's systems in accordance with applicable law. Algolia will comply with this instruction as soon as reasonably practicable within a maximum of 90 days, unless UK, European Union or member state law requires storage.

4.2. Upon expiry of the Term or upon Subscriber's written request, subject to the terms of the Agreement, Algolia shall either (a) return (to the extent such data has not been deleted by Subscriber from the Services) or (b) securely delete Subscriber Data, to the extent allowed by applicable law, in accordance with the timeframes specified in Section 4.3, as applicable.

4.3. Algolia will, after a recovery period of up to 30 days following expiry of the Term, comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless UK, European Union or member state law requires storage. Without prejudice to Section 5 (Data Subject Rights; Data Export), Subscriber acknowledges and agrees that Subscriber will be responsible for exporting, before the Term expires, any Subscriber Data it wishes to retain afterwards.

5. Data Subject Rights; Data Export

5.1. As of the DPA Effective Date for the duration of the period Algolia provides the Services:

5.1.1. Algolia will, in a manner consistent with the functionality of the Services, enable Subscriber to access, rectify and restrict processing of Subscriber Data, including via the deletion functionality provided by Algolia as described in Section 4 (Return or Deletion of Subscriber Data), and to export Subscriber Data;

5.1.2. Algolia will, without undue delay, notify Subscriber, to the extent legally permitted, if Algolia receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure, data portability, objection to the processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"); and

5.1.3. if Algolia receives any request from a data subject in relation to Subscriber Personal Data, Algolia will advise the data subject to submit his or her request to Subscriber and Subscriber will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

5.1.4. Taking into account the nature of the processing, Algolia will assist Subscriber by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of Subscriber's obligation to respond to a Data Subject Request under EU/UK Data Protection Laws. In addition, to the extent Subscriber, in its use of the Services, does not have the ability to address a Data Subject Request, Algolia shall, upon Subscriber's written request, provide Subscriber with reasonable cooperation and assistance to facilitate Subscriber's response to such Data Subject Request, to the extent Algolia is legally permitted to do so and the response to such Data Subject Request is required under EU/UK Data Protection Laws. To the extent legally permitted, Subscriber shall be responsible for any costs arising from Algolia's provision of such assistance.

6. Data Protection Impact Assessment

Upon Subscriber's written request, Algolia will provide Subscriber with reasonable cooperation and assistance needed to fulfill Subscriber's obligation under the GDPR to carry out a data protection impact assessment related to Subscriber's use of the Services, to the extent Subscriber does not otherwise have access to the relevant information, and to the extent such information is available to Algolia. Algolia will provide reasonable assistance to Subscriber in the cooperation or prior consultation with the applicable data protection authority in the performance of its tasks relating to this Section 6 (Data Protection Impact Assessment) to the extent required under EU/UK Data Protection Laws.

7. Sub-processors

7.1. Subscriber specifically authorizes the engagement of Algolia's Affiliates as Sub-processors. In addition, Subscriber acknowledges and agrees that Algolia and Algolia's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Algolia or an Algolia Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Subscriber Data to the extent applicable to the nature of the Services provided by such Sub-processor.

7.2. Algolia will make available to Subscriber the current list of Sub-processors for the Services at https://algolia.com/subprocessors ("**Infrastructure and Sub-processor List**"). Algolia shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to process Subscriber Personal Data in connection with the provision of the Services either by sending an email or via the user interface dashboard of the Services.

7.3. Subscriber may object to Algolia's use of a new Sub-processor by notifying Algolia promptly in writing within ten (10) business days after receipt of Algolia's notice. In the event Subscriber objects to a new Sub-processor, as permitted in the preceding sentence, Algolia will use reasonable efforts to make available to Subscriber a change in the Services or recommend a commercially reasonable change to Subscriber's configuration or use of the Services to avoid processing of Subscriber Personal Data by the objected-to new Sub-processor without unreasonably burdening the Subscriber. If Algolia is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Subscriber may terminate the applicable Service Order(s) with respect to only those Services which cannot be provided by Algolia without the use of the objected-to new Sub-processor by providing written notice to Algolia. Algolia will refund Subscriber any prepaid but unused fees covering the remainder of the term of such Service Order following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Subscriber.

7.4. Algolia shall be liable for the acts and omissions of its Sub-processors to the same extent Algolia would be liable if performing the services of each Sub-processor directly under the terms of this DPA subject to the limitations set forth in Section 10 (Limitation of Liability) and the Agreement.

8. Covered Affiliates

8.1. The parties acknowledge and agree that, by executing the Agreement, the Subscriber enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Covered Affiliates, thereby establishing a separate DPA between Algolia and each such Covered Affiliate subject to the provisions of the Agreement, this Section 8 (Covered Affiliates) and Section 10 (Limitation of Liability). Each Covered Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Covered Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Covered Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Covered Affiliate shall be deemed a violation by Subscriber.

8.2. Subscriber that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Algolia under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Covered Affiliates.

8.3. Where a Covered Affiliate becomes a party to the DPA with Algolia, it shall, to the extent required under applicable Data Protection Laws, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

8.3.1. Except where applicable Data Protection Laws require the Covered Affiliate to exercise a right or seek any remedy under this DPA against Algolia directly by itself, the parties agree that (a) solely Subscriber that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Covered Affiliate, and (b) Subscriber that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Covered Affiliate individually but in a combined manner for all of its Covered Affiliates together (as set forth, for example, in Section 8.3.2 below).

8.3.2. The parties agree that Subscriber that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Subscriber Personal Data, take all reasonable measures to limit any impact on Algolia and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Covered Affiliates in one single audit.

9. Restricted Transfers

9.1. The parties agree that when the transfer of Subscriber Personal Data from Subscriber to Algolia is a Restricted Transfer, it shall be subject to the appropriate Standard Contractual Clauses, as follows:

9.1.1. In relation to Subscriber Personal Data that is protected by the EU GDPR, the EU SCCs will apply as follows:

9.1.1.1. Module Two will apply to the extent that Subscriber is a controller of the Subscriber Personal Data, and Module Three will apply to the extent that Subscriber is a processor of the Subscriber Personal Data on behalf of a third party controller;

9.1.1.2. In Clause 7, the optional docking clause will apply;

9.1.1.3. In Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Clause 7 of this DPA;

9.1.1.4. In Clause 11, the optional language will not apply;

9.1.1.5. In Clause 17, Option 1 will apply, and the EU SCCs will be governed by French law;

9.1.1.6. In Clause 18(b), disputes shall be resolved before the courts of France;

9.1.1.7. Annex I of the EU SCCs shall be deemed completed with (as to Part A) information set out in the Agreement with Subscriber as controller (or processor) and Algolia as processor (or sub-processor), (as to Part B) with the information set out in Attachment 1 to this DPA and (as to Part C) with the supervisory authority set out in Attachment 1 to this DPA;

9.1.1.8. Annex II of the EU SCCs shall be deemed completed with the information set out in Attachment 2 to this DPA;

9.1.1.9. Annex III of the EU SCCs shall be deemed completed with the information set out in Attachment 3 to this DPA;

9.1.2. In relation to Subscriber Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

9.1.2.1. For as long as it is lawfully permitted to rely on standard contractual clauses for the transfer of personal data to processors set out in the European Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of personal data from the United Kingdom, the Prior C2P SCCs shall apply between the Subscriber which, where Subscriber is a processor on behalf of a third party controller, it enters into on behalf of that controller and Algolia, on the following basis:

(A) Appendix 1 shall be completed with the relevant information set out in Attachment 1 to this DPA;

(B) Appendix 2 shall be completed with the relevant information set out in Attachment 2 to this DPA; and

(C) the optional illustrative indemnification Clause will not apply.

9.1.2.2. Where sub-section 9.1.2.1 above does not apply, but the Subscriber and Algolia are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

(A) The EU SCCs, completed as set out above in Section 9.1.1 of this DPA shall also apply to transfers of such Subscriber Personal Data, subject to sub-section (B) below;

(B) The UK Addendum shall be deemed executed between the transferring Subscriber and Algolia, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Subscriber Personal Data.

9.1.2.3. If neither sub-section 9.1.2.1 or sub-section 9.1.2.2 applies, then the Subscriber and Algolia shall cooperate in good faith to implement appropriate safeguards for transfers of such Subscriber Personal Data as required or permitted by the UK GDPR without undue delay.

9.1.3. If any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

9.2. With respect to onward transfers, Algolia shall not participate in (nor permit any Sub-processor to participate in) any other Restricted Transfers of Subscriber Personal Data (whether as an exporter or an importer of the Subscriber Personal Data) unless the Restricted Transfer is made in full compliance with applicable Data Protection Laws and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the Subscriber Personal Data.

10. Limitation of Liability

10.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses, if the Standard Contractual Clauses have been entered into in accordance with the Agreement or a DPA), and all DPAs (including the Standard Contractual Clauses, if the Standard Contractual Clauses have been entered into in accordance with the Agreement or a DPA) between Covered Affiliates and Algolia, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section 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.

10.2. For the avoidance of doubt, Algolia's and its Affiliates' total liability for all claims from the Subscriber and all of its Covered Affiliates arising out of or related to the Agreement and each DPA (including the Standard Contractual Clauses, if the Standard Contractual Clauses have been entered into in accordance with the Agreement or a DPA) shall apply in the aggregate for all claims under both the Agreement and all DPAs (including the Standard Contractual Clauses, if the Standard Contractual Clauses have been entered into in accordance with the Agreement or a DPA) established under this Agreement, including by Subscriber and all Covered Affiliates, and, in particular, shall not be understood to apply individually and severally to Subscriber and/or to any Covered Affiliate that is a contractual party to any such DPA.

10.3. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Attachments and Appendices (including the Standard Contractual Clauses, if the Standard Contractual

Clauses have been entered into in accordance with the Agreement or this DPA).

11. Effect of this DPA

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern.

The parties' authorized signatories have duly executed this Data Processing Agreement as of the date set forth below their respective signatures but made effective as of the DPA Effective Date.

[Signature page follows.]

ALGOLIA SAS

By: DocuSigned by: Julien Lemoine 47CFC113881D43E...

Name: Julien Lemoine

Title: CTO

Date: 9/27/2021

ALGOLIA, INC.

By: DocuSigned by: BN 946262144F1C48F...

Name: Bernadette Nixon

Title: CEO

Date: 9/27/2021

SUBSCRIBER

By: _____

Name: _____

Title: _____

Date: _____

ATTACHMENT 1 TO THE DATA PROCESSING ADDENDUM

DESCRIPTION OF PROCESSING ACTIVITIES

Categories of data subjects whose personal data is transferred:	Data subjects include the individuals about whom personal data is provided to Algolia via the Services by (or at the direction of) Subscriber or by Subscriber's end users, the extent of which is determined and controlled by the Subscriber in its sole discretion, and which may include but is not limited to personal data relating to the following categories of data subjects: 1. **Service Administrators** a. Employees or contractors of Subscriber, Subscriber's Affiliates, customers, business partners and vendors having access to the Algolia dashboard (who are natural persons) b. Agents, advisors, freelancers of Subscriber having access to the Algolia dashboard (who are natural persons) 2. **Subscriber' End Users** a. Subscriber's users interacting with the Services (who are natural persons) ("**End Users**")
Categories of personal data transferred:	Personal data relating to individuals provided to Algolia via the Services, by (or at the direction of) Subscriber or by Subscriber's end users, the extent of which is determined and controlled by Subscriber in its sole discretion, and which may include but is not limited to personal data relating to the following categories of data: 1. **Service Administrator's Data** a. First, Middle and Last Name (current and former) b. Title or position c. Employer d. Personal and Business Contact Information (company, email, physical address, phone number) e. Network connection data f. IP address g. Location of request (as indicated in IP address) 2. **End User Data** a. IP address b. User statistics through the search function c. Network connection data d. Location of request (as indicated in IP address)
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions, keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Subscriber may submit special categories of data to the Service as a part of its Subscriber Data, the extent of which is determined and controlled by Subscriber in its sole discretion, and which is for the sake of clarity personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, and the processing of data concerning health or sex life. Security measures are set out in Attachment 2.
The frequency of the transfer:	Continuous.
Nature of the processing:	Algolia provides site services on a SaaS model, accessible through API.
Purpose(s) of the data transfer and further processing:	The purpose of the data processing under this DPA is the provision of Algolia Services to the Subscriber and the performance of Algolia's

	obligations under the Agreement or as otherwise agreed by the parties.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Until 90 days after termination and expiry of the Agreement. Personal Data is purged from Algolia's systems on a rolling 90-day period, starting the day after termination, with the latest collected data being purged on day 90.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Where Algolia engages Processors (or sub-Processors) it will do so in compliance with the terms of any applicable Standard Contractual Clauses. The subject matter, nature and duration of the Processing activities carried out by the Processor (or sub-Processor) will not exceed the subject matter, nature and duration of the Processing activities as described in this Attachment. The list of approved sub-Processors is available at https://www.algolia.com/policies/infrastructure-and-sub-processors/.

SUPERVISORY AUTHORITY

Supervisory Authority	The supervisory authority of **France** shall act as competent supervisory authority.

ATTACHMENT 2 TO THE DATA PROCESSING ADDENDUM

SECURITY MEASURES

Algolia implements and maintains Security Measures that meet or exceed the security objectives required for SOC2 audit. Algolia may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. These Security Measures are in effect on the DPA Effective Date. Capitalized terms used herein but not otherwise defined have the meaning given to them in the DPA.

Information Security Program

1) Data Center and Network Security

a) Data Centers

i) **Infrastructure**. Algolia maintains geographically distributed data centers and stores all production data in physically secure data centers.

ii) **Redundancy**. Algolia's infrastructure has been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. This design allows Algolia to perform maintenance and improvements of the infrastructure with minimal impact on the production systems. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications.

iii) **Power**. All data centers are equipped with redundant power system with various mechanism to provide backup power, such as uninterruptible power supplies (UPS) batteries for short term blackouts, over voltage, under voltage or any power instabilities and diesel generators, for outages extending units of minutes, which allow the data centers to operate for days.

iv) **Server Operating System**. Algolia uses a Linux based operating system for the application environment with a centrally managed configuration. Algolia has established a policy to keep systems up to date with necessary security updates.

v) **Business Continuity**. Algolia replicates data across multiple systems to help protect against accidental destruction or loss. Algolia has designed and regularly plans and tests its business continuity planning and disaster recovery programs.

b) Network and Transmission

i) **Data Transmission**. Algolia uses industry standard encryption schemes and protocols to encrypt data transmissions between the data centers. This is intended to prevent reading, copying or modification of the data.

ii) **Intrusion Detection**. Algolia employs an intrusion detection system to provide insights into ongoing attack activities and to help remediate the attack faster.

iii) **Incident Response**. Algolia's security and operations personnel will promptly react to discovered security incidents and inform the involved parties.

iv) **Encryption Technologies**. Algolia's servers support HTTPS encryption, ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA and for supported clients also perfect forward secrecy (PFS) methods to help protect traffic against compromised key or cryptographic breakthrough. Algolia uses only industry standard encryption technologies.

2) Access and Site Controls

a) Site Controls

i) **Data Center Security Operations**. All data centers in use by Algolia maintain 24/7 on-site security operations responsible for all the aspects of physical data center security.

ii) **Data Center Access Procedures**. Access to the datacenter follows Algolia's Physical Security policy allowing only pre-approved authorized personnel to access the Algolia equipment.

iii) **Data Center Security**. All data centers comply with or exceed the security requirements of SOC2. All data centers are equipped with CCTV, on-site security personnel and key card access system.

b) Access Control

i) **Access Control and Privilege Management**. Subscriber's administrators must authenticate themselves via a central authentication system or via a single sign-on system in order to administer the Services.

ii) **Internal Data Access Processes and Policies – Access Policy**. Algolia's internal data access processes

and policies are designed to prevent unauthorized persons or systems from getting access to systems used to process personal data. These processes are audited by an independent auditor. Algolia employs a centralized access management system to control access to production systems and servers, and only provides access to a limited number of authorized personnel. SSO, LDAP and SSH certificates are used to provide secure access mechanisms. Algolia requires the use of unique IDs, strong passwords and two factor authentication. Granting of access is guided by an internal policy. Access to the system is logged to provide an audit trail for accountability.

3) **Data**
   a) **Data Storage, Isolation and Logging**. Algolia stores data in a combination of dedicated and multi-tenant environments on Algolia-controlled servers. The data is replicated on multiple redundant systems. Algolia also logically isolates the Subscriber's data. Subscriber may enable data sharing, should the Services functionality allow it. Subscriber may choose to make use of certain logging capability that Algolia may make available via the Services.
   b) **Decommissioned Disks and Disk Erase Policy**. Disks used in servers might experience hardware failures, performance issues or errors that lead to their decommission. All decommissioned disks are securely erased if intended for reuse, or securely destroyed due to malfunction.

2) **Personnel Security**
   Algolia personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Algolia conducts appropriate background checks to the extent allowed by applicable law and regulations. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Algolia's confidentiality, privacy and acceptable use policies. All personnel are provided with security training upon employment and then regularly afterwards. Algolia's personnel will not process Subscriber Data without authorization.

3) **Sub-processor Security**
   Algolia conducts audits of security and privacy practices of Sub-processors prior to onboarding the Sub-processors in order to ensure adequate level of security and privacy to data and scope of services they are engaged to provide. Once the Sub-processor audit is performed and associated risk is evaluated, the Sub-processor enters into appropriate privacy, confidentiality and security contract terms.

Security Certifications and Reports

1) **Service Organization Control (SOC) Reports**: Currently, Algolia's information security control environment applicable to the Services undergoes an independent evaluation in the form of SOC2 and SOC 3 audits. To demonstrate compliance with the Security Measures, Algolia will make available for review by Subscriber Algolia's most recent (i) SOC 2 Report and (ii) SOC 3 Report as described below.
   a. **"SOC 2 Report"** means a confidential Service Organization Control (SOC) 2 report on Algolia's systems examining logical security controls, physical security controls, and system availability, as produced by Algolia's independent third-party auditor in relation to the Services.
   b. **"SOC 3 Report"** means a Service Organization Control (SOC) 3 report, as produced by Algolia's independent third-party auditor in relation to the Services**.**
   c. Algolia will either update the SOC2 Report and SOC 3 Report at least once every 18 months or pursue comparable audits or certifications to evaluate and help ensure the continued effectiveness of the Security Measures.

1) **ISO27001 and ISO27017 certification:** In March 2020, Algolia received its ISO27001 and ISO27017 certifications which are an information security management system family of standards providing best practice recommendations on information security management, including framework of policies and procedures that include all legal, physical and technical controls involved in an organization's information management process, and security standards particularly developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security issues, respectively.
2) **TRUSTe certification**: Algolia has been awarded the TRUSTe Certified Seal signifying that Algolia's website Privacy Statement and privacy practices related to the Services have been reviewed by TRUSTe for compliance with TRUSTe's Certification Standards.

ATTACHMENT 3 TO THE DATA PROCESSING ADDENDUM

ADDENDUM FOR SUBSCRIBERS LOCATED IN THE EEA OR UK

Notwithstanding anything to the contrary set forth in the DPA, Subscriber's End User Data, as described in Attachment 1 to the DPA, will not be sent outside of the EEA or the United Kingdom, provided that Subscriber meets the following requirements and/or obligations (i) Subscriber keeps its services located in the EEA or the United Kingdom, as applicable, (ii) End-Users do not access the Algolia Insights Services from outside of the EEA or the United Kingdom, as applicable (e.g. Automated Personalization), and (iii) Subscriber or Subscribers' End Users do not violate the Agreement, including the Acceptable Use Policy, or use the Services in a way that triggers a security incident resulting in the activation of Algolia's security review procedures. In such case, the IP address of the End User may be sent to a security watchlist in a country that offers an adequate level of data protection and retained for 12 months for security incident handling. Notwithstanding anything to the contrary set forth herein, EEA/UK based End User Data processed for the analytics features are hosted by default in the EEA/UK.