# Data Processing Addendum

This Data Processing Addendum ("**DPA**") 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 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.

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 Algolia, Inc., a company incorporated in Delaware, Algolia SAS, a French société par actions simplifiées or Algolia Limited, a company registered in England and Wales, or any other Algolia Affiliate that is a party to the Agreement, as applicable.

"**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 Data Protection Laws.

"**DPA Effective Date**" means, as applicable, (a) May 25, 2018 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 May 25, 2018.

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

"**EU Data Protection Laws**" means laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the processing of Personal Data under the Agreement, including European Directives 95/46/EC and any legislation and/or regulation which amends, replaces or re-enacts it (including the GDPR).

"**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 effective as of May 25, 2018 and any legislation and/or regulation which amends, replaces or re-enacts it.

"**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 administrative, technical and physical safeguards adopted by Algolia applicable to the Services subscribed by Subscriber as described and made available at https://www.algolia.com/security or as otherwise made available by Algolia. The Security Measures as of April 25, 2018 is attached to this DPA as Attachment 2.

**"Standard Contractual Clauses"** means the agreement executed by and between Subscriber and Algolia, Inc. attached hereto as Attachment 3, pursuant to the European Commission's decision (C(2010)593) 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.

"**Sub-processor**" means any third-party engaged by Algolia or a member of the Algolia Group which processes Subscriber Data in order to provide parts of the Services.

"**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 GDPR, 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 Data Protection Laws apply to the processing of Subscriber Personal Data, the parties acknowledge and agree that:

2.1.1. Subscriber is the controller and Algolia and the Algolia Group are the processor of the Subscriber Personal Data and Algolia or a member of the Algolia Group may engage Sub-processors pursuant to Section 7 (Sub-processors).

2.1.2. 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.

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

2.1.4. If the GDPR is applicable, Algolia will process Subscriber Personal Data in accordance with the requirements of the GDPR directly applicable to Algolia's provision of Services. Notwithstanding anything to the contrary set forth in this DPA, in the event of a conflict or clarification of definitions, the GDPR shall apply only as of May 25, 2018.

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 another 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 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.

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 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 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.

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 the Algolia Group'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 the 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 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 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 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 the GDPR.

**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 ("**Infrastructure and Sub-processor List**"). The Infrastructure and Sub-processor List as of the DPA Effective Date is attached as Appendix 3 of the Standard Contractual Clauses (which is attached hereto as Attachment 3). Such Sub-processor list will include the identities of those Sub-processors and their corporate location. Subscriber may find the most current Infrastructure and Sub-processor List at https://algolia.com/subprocessors (under the "Infrastructure and Sub-Processor List" link). 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. Transfer of Personal Data outside of the EEA**

9.1. Algolia makes the Standard Contractual Clauses available as a transfer mechanism for any transfer of Subscriber Personal Data under this DPA from the European Union, the EEA and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of EU Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws.

9.2. The Standard Contractual Clauses and the additional terms specified in this Section 9 (Transfer of Personal Data Outside of the EEA) apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Covered Affiliates and (ii) all Affiliates of Subscriber established within the EEA, Switzerland and the United Kingdom, which have signed Service Orders for Services. For the purpose of the Standard Contractual Clauses and this Section 9, all these entities shall be deemed “data exporters”.

9.3. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the 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.

9.4. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Subscriber acknowledges and expressly agrees that (a) Algolia’s Affiliates may be retained as Sub-processors; and (b) Algolia and Algolia’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Algolia will make available to Subscriber the current list of Sub-processors in accordance with Section 7 (Sub-processors).

9.5. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Subscriber acknowledges and expressly agrees that Algolia and Algolia’s Affiliates may engage new Sub-processors as described in Sections 7 (Sub-processors).

9.6. The parties agree that the copies of the Sub-processor agreements that must be provided by Algolia to Subscriber pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Algolia beforehand; and, that such copies will be provided by Algolia, in a manner to be determined in its discretion, only upon request by Subscriber.

9.7. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

9.7.1. Upon Subscriber's written request, at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Algolia shall 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 the Algolia Group's compliance with the obligations set forth in this DPA 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. 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 Personal 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.

9.8. The parties agree that the certification of deletion of Subscriber Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Algolia to Subscriber only upon Subscriber's written request.

9.9. In the event of any conflict or inconsistency between the body of this DPA and any of its attachments (not including the Standard Contractual Clauses) and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

9.10. In the event that the European Commission decision authorizing the Standard Contractual Clauses as a data transfer mechanism is held to be invalid, or that any supervisory authority requires transfer of Personal Data made pursuant to such decision to be suspended, then Subscriber may, at its discretion, require Algolia to cease processing Subscriber Personal Data to which this Section 9 applies, or co-operate with Algolia to facilitate use of an alternative transfer mechanism.

9.11. Algolia agrees to comply with the obligations of a data importer as set out in the Standard Contractual Clauses for the transfer of Subscriber Personal Data to data processors established in third countries under the Standard Contractual Clauses.

9.12. Subscriber acknowledges that Algolia will, as applicable, be a data importer under the Standard Contractual Clauses. In particular, and without limiting the above obligation:

9.12.1. Algolia agrees to grant third-party beneficiary rights to data subjects, as set out in Clause 3 of the Standard Contractual Clauses, provided that Algolia's liability shall be limited to Algolia's own processing operations only and the limitations set forth in Section 10 (Limitation of Liability) and the Agreement; and

9.12.2. Algolia agrees that Algolia's obligations under the Standard Contractual Clauses shall be governed by the law(s) of the EEA member state(s) in which the entity that is the data exporter is established.

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.]

| | |
|---|---|
| **[SUBSCRIBER ENTITY NAME]** | **ALGOLIA, INC.** |
| By: | By: DocuSigned by: Nicolas Dessaigne 9EE657E82EF9478... |
| Name: | Name: Nicolas Dessaigne |
| Title: | Title: Co-founder & Chief Executive Officer |
| Date: | Date: 4/24/2018 |

| | |
|---|---|
| **ALGOLIA SAS** | **ALGOLIA LIMITED** |
| By: DocuSigned by: Julien Lemoine 47CFC113881D43E... | By: DocuSigned by: Nicolas Dessaigne 9EE657E82EF9478... |
| Name: Julien Lemoine | Name: Nicolas Dessaigne |
| Title: Co-founder, Chief Technology Officer and President Directeur General | Title: Director |
| Date: 24/04/2018 | Date: 4/24/2018 |

| |
|---|
| By: DocuSigned by: Julien Lemoine 47CFC113881D43E... |
| Name: Julien Lemoine |
| Title: Director |
| Date: 24/04/2018 |

# ATTACHMENT 1 TO THE DATA PROCESSING ADDENDUM

## DESCRIPTION OF PROCESSING ACTIVITIES

**Data subjects**
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. Prospects, customers, business partners and vendors of Subscriber (who are natural persons)
2. Employees or contact persons of Subscriber's prospects, customers, business partners and vendors (who are natural persons)
3. Employees, agents, advisors, freelancers of Subscriber (who are natural persons)
4. Subscriber's users authorized by Subscriber to use the Services (who are natural persons)

**Categories of data**
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. First, Middle and Last Name (current and former)
2. Title
3. Position
4. Employer
5. Personal and Business Contact Information (company, email, physical address, phone number)
6. ID data
7. Professional life data
8. Personal life data
9. Connection data
10. Localization data

**Special categories of data**
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, and the processing of data concerning health or sex life.

**Processing operations**
Subscriber Personal Data will be processed in accordance with the Agreement and this DPA.

# 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 certification. 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 system to help protect against accidental destruction of 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 Intrusion detection system to provide insight into ongoing attack activities and to help remediate the attack faster.
      iii) **Incident Response**. Algolia's security 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 system 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 server, 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 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 environment 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 issue or errors that lead to their decommission. All decommissioned disk are securely erased if intended for reuse, or securely destroyed due to malfunction.

4) **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 backgrounds 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.

5) **Sub-processor Security**

Algolia conducts audit 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.

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

## STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
**Unit C.3: Data protection**

**Commission Decision C(2010)593**
**Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: _____

Address: _____

Tel.:……; fax……; e-mail:……

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organisation: Algolia, Inc.
Address: 589 Howard Street Suite 5, San Francisco, California 94105, U.S.A.

(the data **importer**)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1*

***Definitions***

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law***'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*

***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4*

***Obligations of the data exporter***

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and,

where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

*Clause 5*

***Obligations of the data importer***

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body

composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

*Clause 6*

***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

*Clause 7*

***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any

subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10*

***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*

***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**DATA EXPORTER**

Name**:** _____

By: Name (written out in full): _____

Position: _____

Address: _____

Signature…….
(stamp of organisation)

Date……

**DATA IMPORTER**

Name**:** Algolia, Inc.

By: Name (written out in full): Nicolas Dessaigne

Position: Co-founder & Chief Executive Officer

Address: 589 Howard Street Suite 5 San Francisco, California 94105

DocuSigned by:
Nicolas Dessaigne
9EE657E82EF9478...

Signature…….
(stamp of organisation)

4/24/2018

Date……

# APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data Exporter**
The data exporter is _____, the Subscriber or Subscriber in the Algolia subscription documents (herein referred to as the "**Subscriber**").

**Data Importer**
The data importer is Algolia, Inc. ("**Algolia**"), a hosted search services provider.

**Data subjects**
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. Prospects, customers, business partners and vendors of Subscriber (who are natural persons)
2. Employees or contact persons of Subscriber's prospects, customers, business partners and vendors (who are natural persons)
3. Employees, agents, advisors, freelancers of Subscriber (who are natural persons)
4. Subscriber's users authorized by Subscriber to use the Services (who are natural persons)

**Categories of data**
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. First, Middle and Last Name (current and former)
2. Title
3. Position
4. Employer
5. Personal and Business Contact Information (company, email, physical address, phone number)
6. ID data
7. Professional life data
8. Personal life data
9. Connection data
10. Localization data

**Special categories of data**
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, and the processing of data concerning health or sex life.

**Processing operations**
Subscriber Personal Data will be processed in accordance with the Agreement and this DPA.

**DATA EXPORTER**

Name**:** _____

By: Name (written out in full): _____

Position: _____

Address: _____

Signature…….
(stamp of organisation)

Date……

**DATA IMPORTER**

Name**:** Algolia, Inc.

By: Name (written out in full): Nicolas Dessaigne

Position: Co-founder & Chief Executive Officer

Address: 589 Howard Street Suite 5, San Francisco, California 94105, U.S.A.

DocuSigned by:
Nicolas Dessaigne
9EE657E82EF9478...

Signature…….
(stamp of organisation)

4/24/2018

Date……

# APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Data importer will maintain administrative, technical and physical safeguards designed to protect the security, confidentiality and integrity of personal data submitted to the subscribed services as described in the applicable Security Measures described at https://www.algolia.com/security or otherwise made reasonably available by data importer. The Security Measures as of April 25, 2018 are attached to the DPA as Attachment 2.

**DATA EXPORTER**

Name: _____

By: Name (written out in full): _____

Position: _____

Address: _____

Signature.....
(stamp of organisation)

Date.....

**DATA IMPORTER**

Name: Algolia, Inc.

By: Name (written out in full): Nicolas Dessaigne

Position: Co-founder & Chief Executive Officer

Address: 589 Howard Street Suite 5, San Francisco, California 94105, U.S.A.

DocuSigned by:
Nicolas Dessaigne
9EE657E82EF9478...

Signature.....
(stamp of organisation)

4/24/2018

Date.....

# APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

## INFRASTRUCTURE AND SUB-PROCESSOR LIST

### Infrastructure Sub-processors

Algolia operates worldwide infrastructure in co-location and server hosting facilities of our infrastructure partners together with industry leading cloud service providers. Algolia owns and controls logical access to the infrastructure maintained by the entities set forth below, while these entities maintain the physical security of the servers, network and the data center.

| Entity Name | Entity Type | Corporate Location |
|---|---|---|
| **Amazon Web Services, Inc.** | Cloud Service Provider | United States |
| **Google LLC** | Cloud Service Provider | United States |
| **LeaseWeb Global B.V.** | Server Provider | Netherlands |
| **OVH SAS** | Server Provider | France |
| **IPTP Networks** | Server Provider | Netherlands |
| **Hetzner Online GmbH** | Server Provider | Germany |
| **Anexia Internetdienstleistungen GmbH** | Server Provider | Austria |
| **WANSecurity Inc.** | Server Provider | United States |
| **Internap Corporation** | Server Provider | United States |
| **Packet Host, Inc.** | Server Provider | United States |
| **Zone Networks Pty Ltd.** | Server Provider | Australia |
| **E2E Networks Private Limited** | Server Provider | India |
| **WebWerks India Pvt. Ltd.** | Server Provider | India |
| **MaxiHost LTDA.** | Server Provider | Brazil |
| **Danidin Ltd.** | Server Provider | Cyprus |
| **Equinix, Inc.** | Data Center | United States |

### Service Specific Sub-processors

Algolia works with certain third-parties to provide a specific functionality within its Services. These third-parties are Sub-processors with limited use indicated below and access to Subscriber Data in order to provide the relevant functionality.

| Entity Name | Purpose | Corporate Location |
|---|---|---|
| **Citus Data, Inc.** | Citus Data provides a hosted PostreSQL database used for our Analytics services. The primary information Citus Data has access to: search queries, end-user IP address. | United States |
| **Cloudflare, Inc.** | Cloudflare provides content distribution (CDN), security and DNS services for web traffic to and from the services. The primary information Cloudflare has access to is information in and associated with the Algolia website URL that the end-user is interacting with (which includes end-user IP address). | United States |

### Algolia Group Sub-processors

The following entities are the current members of the Algolia Group. Accordingly, they function as sub-processors to provide the Services.

| Entity Name | Country |
|---|---|
| **Algolia, Inc.** | United States |
| **Algolia SAS** | France |
| **Algolia Limited** | United Kingdom |