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

The entity, individual or organization who accesses or uses the Algolia Services
(the data **exporter**)

And

Name of the data importing organisation:

Algolia, Inc.

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

Tel.: [1](415) 366-9672

e-mail: contact@algolia.com

(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.

On behalf of the data exporter:

Agreed to by the data exporter by accessing or using the Algolia Services.

On behalf of the data importer:

Name (written out in full): Nicolas Dessaigne

Position: CEO

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

Signature……Nicolas Dessaigne……

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 (please specify briefly your activities relevant to the transfer):
transferring the data to the data importer in connection with the data exporter's use of the data importer's data transformation software.

Data importer
The data importer is a provider of data transformation software in a hosted environment.

Data subjects
The personal data transferred may concern data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Categories of data
The data exporter shall identify to the data importer any categories of personal data transferred.

Processing operations
The personal data transferred will be subject to the following basic processing activities:
Analysis and data transformation using data importer's data transformation software.

DATA EXPORTER

Agreed to by the data exporter by accessing or using the Algolia Services.

DATA IMPORTER

Name: Algolia, Inc.

Authorised Signature ……………………… Nicolas Dessaigne

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

1. Technical and Organizational Measures. The following sections define the current security measures established by Algolia. Algolia may change these at any time without notice by keeping a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.
    a. Physical Access Control: Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which process and/or use Personal Data.:
        i. All data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To ensure proper functionality, physical security equipment (e.g. motion sensors, cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at all data centers:
        ii. Algolia protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
        iii. In general, buildings are secured through access control systems (smart card access system).
        iv. As a minimum requirement, the outermost shell of the building must be fitted with a certified key system including modern, active key management.
        v. Depending on the security classification, buildings, individual areas and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
        vi. Access rights will be granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.b and 1.c below). This also applies to visitor access. Guests and visitors to Algolia buildings must register their names at reception and must be accompanied by authorized Algolia personnel. Algolia and all third party data center providers are logging the names and times of persons entering the private areas of Algolia within the data centers.
    b. System Access Control: Data processing systems used to provide the Algolia Services must be prevented from being used without authorization.:
        i. Multiple authorization levels are used to grant access to sensitive systems including those storing and processing Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
        ii. All users access Algolia's systems with a unique identifier (user ID).
        iii. Algolia has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, its access rights are revoked.
        iv. Algolia has established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In case of domain passwords, the system forces a password change every six months complying with the requirements for complex passwords. Each computer has a password-protected screensaver.
        v. The company network is protected from the public network by firewalls.
        vi. Algolia uses up–to-date antivirus software at access points to the company network (for e-mail accounts) and on all file servers and all workstations.
        vii. A security patch management is implemented to ensure deployment of relevant security updates.
        viii. Full remote access to Algolia's corporate network and critical infrastructure is protected by strong authentication.
    c. Data Access Control: Persons entitled to use data processing systems shall gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.:

    i. Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. Algolia uses authorization concepts that document how authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the Algolia security policies and standards.
    ii. All production servers of any Algolia Services are operated in the relevant data centers/server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, Algolia conducts internal and external security checks and penetration tests on the IT systems.
    iii. Algolia does not allow the installation of personal software or other software not approved by Algolia to systems being used for any Algolia Services.
    iv. A Algolia security standard governs how data and data carriers are deleted or destroyed.

d. Data Transmission Control: Personal Data must not be read, copied, modified or removed without authorization during transfer.:
    i. Where data carriers are physically transported, adequate measures are implemented at Algolia to ensure the agreed service levels (for example, encryption, and lead-lined containers).
    ii. Personal Data transfer over Algolia internal networks are protected as any other confidential data according to Algolia Security Policy.
    iii. When the data is being transferred between Algolia and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the Agreement. This applies to both physical and network based data transfer. In any case the Customer assumes responsibility for any data transfer from Algolia's Point of Demarcation (e.g. outgoing firewall of the Algolia data center which hosts the Algolia Services).

e. Data Input Control: It shall be possible to retrospectively examine and establish whether and by whom at Algolia Personal Data have been entered, modified or removed from data processing systems used to provide the Algolia Services.:
    i. Algolia only allows authorized persons to access Personal Data as required in the course of their work. Algolia implemented a logging system for input, modification and deletion, or blocking of Personal Data by Algolia or its Subprocessors to the greatest extent supported by the Algolia Services.

f. Job Control: Personal Data being processed on commission shall be processed solely in accordance with the Agreement and related instructions of the Customer.:
    i. Algolia uses controls and processes to ensure compliance with contracts between Algolia and its customers, Subprocessors or other service providers.
    ii. As part of the Algolia Security Policy, Customer Data requires at least the same protection level as "confidential" information.
    iii. All Algolia employees and contractual partners are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Algolia customers and partners.

g. Availability Control: Personal Data shall be protected against accidental or unauthorized destruction or loss.:
    i. Algolia employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
    ii. Algolia uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the data centers.
    iii. Algolia has defined contingency plans as well as business and disaster recovery strategies for Algolia Services.
    iv. Emergency processes and systems are regularly tested.

h. Data Separation Control: Personal Data collected for different purposes can be processed separately.:
    i. Algolia uses the technical capabilities of the deployed software to achieve data separation between Personal Data from one and any other customer.
    ii. Algolia maintains dedicated instances for each Customer.
    iii. Customers have access only to their own Customer instance(s).

i. Data Integrity Control: Ensures that Personal Data will remain intact, complete and current during processing activities:
    i. Algolia has implemented a defense strategy in several layers as a protection against unauthorized modifications.

ii. This refers to controls as stated in the control and measure sections as described above. In particular:

    1. Firewalls;
    2. Security Monitoring Center;
    3. Antivirus software;
    4. Backup and recovery; and
    5. External and internal penetration testing.