



**Note to copy:**

*The HubSpot Data Processing Agreement is made available at <https://legal.hubspot.com/dpa> and is incorporated into the HubSpot Customer Terms of Service available at <https://legal.hubspot.com/terms-of-service>, as specified in the HubSpot Customer Terms of Service.*

*For Customers that would like to receive a signed copy of the HubSpot Data Processing Agreement, we have made this copy available to you. This copy includes signatures on the Data Processing Agreement version last modified November 1, 2018. No changes made to this copy are agreed to by HubSpot, Inc. or its affiliates.*

*Please note that we update the Data Processing Agreement as we describe in the 'General Provisions' section below. Current Data Processing Agreement terms are available at <https://legal.hubspot.com/dpa> and archived Data Processing Agreement terms are available at <https://legal.hubspot.com/legal-stuff/archive>.*

*If you have any questions, please contact your HubSpot representative.*

## HubSpot Data Processing Agreement

Last Modified: November 1, 2018

This HubSpot Data Processing Agreement (“DPA”), that includes the Standard Contractual Clauses adopted by the European Commission, as applicable, reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under the [HubSpot Customer Terms of Service](#) (the “Agreement”). This DPA is an amendment to the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order or an executed amendment to the Agreement. Upon its incorporation into the Agreement, the DPA will form a part of the Agreement.

We periodically update these terms. If you have an active HubSpot subscription, we will let you know when we do via an email or in-app notification. You can find archived versions of the terms [here](#).

The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. [Definitions](#)
2. [Details of the Processing](#)
3. [Controller Responsibility](#)

4. [Obligations of Processor](#)
5. [Data Subject Requests](#)
6. [Audits](#)
7. [Sub-Processors](#)
8. [Data Transfers](#)
9. [General Provisions](#)
10. [Parties to this DPA](#)

## [EXHIBIT 1](#)

### [Appendix 1 to the Standard Contractual Clauses](#)

### [Appendix 2 to the Standard Contractual Clauses](#)

The HubSpot Sub-Processors Page found [here](#), which includes a list of the sub-Processors we use in connection with the provision of the Subscription Service.

#### **1. Definitions**

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Protection Law” means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms “process”, “processes” and “processed” will be construed accordingly.

“Data Subject” means the individual to whom Personal Data relates.

“GDPR” means the General Data Protection 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.

“Instruction” means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as

personal data or personally identifiable information under applicable Data Protection Law.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

“Processor” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the clauses attached hereto as Exhibit 1 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-Processors Page” means HubSpot’s Sub-Processors Page available at <https://legal.hubspot.com/sub-processors-page>.

## **2. Details of the Processing**

a. Categories of Data Subjects. Controller may submit Personal Data to the Subscription Service, the extent of which is determined and controlled by Controller in its sole discretion, and which may include, but is not limited to Controller’s Contacts and other end users including Controller’s employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller’s end users.

b. Types of Personal Data. Contact Information (as defined in the HubSpot Customer Terms of Service), the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by the Controller, or the Controller’s end users, via the Subscription Service.

c. Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the provision of the services to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order.

d. Purpose of the Processing. Personal Data will be Processed for purposes of providing the services set out, as further instructed by Controller in its use of the Services, and otherwise agreed to in the Agreement and any applicable Order.

e. Duration of the Processing. Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

### **3. Controller Responsibility**

Within the scope of the Agreement and in its use of the services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with the Data Protection Law. This DPA is Customer's complete and final instruction to HubSpot in relation to Personal Data and that additional instructions outside the scope of DPA would require prior written agreement between the parties. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (as individual instructions).

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

### **4. Obligations of Processor**

a. Compliance with Instructions. The parties acknowledge and agree that Customer is the Controller of Personal Data and HubSpot is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable European Union or Member State law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

b. Security. Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under Appendix 2 to the Standard Contractual Clauses. Such measures include, but are not limited to:

i. the prevention of unauthorized persons from gaining access to Personal Data Processing systems,

- ii. the prevention of Personal Data Processing systems from being used without authorization,
- iii. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization,
- iv. ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified,
- v. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems,
- vi. ensuring that Personal Data is Processed solely in accordance with the Instructions,
- vii. ensuring that Personal Data is protected against accidental destruction or loss.

Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by (i) implementing and maintaining the security measures described under Appendix 2, (ii) complying with the terms of Section 4.d. (Personal Data Breaches); and (iii) providing the Controller with information in relation to the Processing in accordance with Section 6 (Audits).

c. Confidentiality. Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

d. Personal Data Breaches. Processor will notify the Controller without undue delay after it becomes aware of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

e. Deletion or Retrieval of Personal Data. Other than to the extent required to comply with Data Protection Law, following termination or expiration of the Agreement, Processor will delete or return all Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Controller.

Processor will enable Controller to delete Personal Data of end users using the functionality of the Subscription Service.

f. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is available to Processor and the Controller does not otherwise have access to the required information, Processor will provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to the processing of Personal Data.

## **5. Data Subject Requests**

Processor will enable Controller to respond to requests from Data Subjects to exercise their rights under the applicable Data Protection Law in a manner consistent with the functionality of the Subscription Service. To the extent that Controller does not have the ability to address a Data Subject request, then upon Controller's request Processor shall provide reasonable assistance to the Controller to facilitate such Data Subject request to the extent able and only as required by applicable Data Protection Law. Controller shall reimburse Processor for the commercially reasonable costs arising from this assistance.

Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests.

## **6. Audits**

Processor shall, in accordance with Data Protection Laws and in response to a reasonable written request by Controller, make available to Controller such information in Processor's possession or control related to Processor's compliance with the obligations of data processors under Data Protection Law in relation to its Processing of Personal Data.

Controller may, upon written request and at least 30 days' notice to Processor, during regular business hours and without interrupting Processor's business operations, conduct an inspection of Processor's business operations or have the same conducted by a qualified third party auditor subject to Processor's approval, which shall not be unreasonably withheld.

Processor shall, upon Controller's written request and on at least 30 days' notice to the Processor, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

## **7. Sub-Processors**

a. Appointment of Sub-Processors. Controller acknowledges and agrees to (a) the engagement as sub-Processors of Processor's affiliated companies and the third parties listed on our Sub-Processors Page, and (b) that Processor and Processor's affiliated companies respectively may engage third-party sub-Processors in connection with the provision of the Subscription Service. For the avoidance of doubt, the above authorization constitutes Controller's prior written consent to the sub-Processing by Processor for purposes of Clause 11 of the Standard Contractual Clauses.

Where Processor engages sub-Processors, Processor will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA. Where the sub-Processor fails to fulfill its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processors obligations.

Where a sub-Processor is engaged, the Controller must be granted the right to monitor and inspect the sub-Processor's activities in accordance with this DPA and the Data Protection Law, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-Processing contract, where necessary by inspecting the relevant contract documents.

The provisions of this Section 7 shall mutually apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this DPA, HubSpot transfers any Personal Data to a sub-Processor located outside of the EEA, HubSpot shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

b. Current Processor List and Notification or Objection to New Sub-Processors. If the Processor intends to instruct sub-Processors other than the companies listed on the Sub-Processors Page, the Processor will notify the Controller by updating the Sub-

Processors Page and will give the Controller the opportunity to object to the engagement of the new sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds. If the Processor and Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party. Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination. If the Controller would like to receive an email notification when we update the Sub-Processors Page, complete the form found [here](#).

## **8. Data Transfers**

Controller acknowledges and agrees that, in connection with the performance of the services under the Agreement, Personal Data will be transferred to HubSpot, Inc. in the United States. Processor may access and perform Processing of Personal Data on a global basis as necessary to provide the Subscription Service, in accordance with the HubSpot Customer Terms of Service.

HubSpot, Inc. has certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as administered by the U.S. Department of Commerce, in order to implement appropriate safeguards for such transfers pursuant to Article 46 of the GDPR. The Standard Contractual Clauses at Exhibit 1 will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Law).

To the extent that Controller or Processor are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently revoked, or held in a court of competent jurisdiction to be invalid, Controller and Processor agree to cooperate in good faith to pursue a suitable alternate mechanism that can lawfully support the transfer.

## **9. General Provisions**

With respect to updates and changes to this DPA, the terms that apply in the "Amendment; No Waiver" section of "Miscellaneous" in the Agreement shall apply.

In case of any conflict, this DPA shall take precedence over the regulations of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

Upon the incorporation of this DPA into the Agreement, the parties indicated in Section 10 below (Parties to this DPA) are agreeing to the Standard Contractual Clauses (where and as applicable) and all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Exhibit 1, the Standard Contractual Clauses shall prevail, provided however: (a) Controller may exercise its right of audit under clause 5(f) of the standard contractual clauses as set out in, and subject to the requirements of, section 6 of this DPA; and (b) Processor may



appoint sub-Processors as set out, and subject to the requirements of, section 4 and section 7 of this DPA.

#### **10. Parties to this DPA**

This DPA is an amendment to and forms part of the Agreement. Upon the incorporation of this DPA into the Agreement (i) Controller and the HubSpot entity that are each a party to the Agreement are also each a party to this DPA, and (ii) to the extent that HubSpot Inc. is not the party to the Agreement, HubSpot, Inc. is a party to this DPA, but only with respect to agreement to the Standard Contractual Clauses of the DPA, this Section 10 of the DPA, and to the Standard Contractual Clauses themselves.

If HubSpot, Inc. is not a party to the Agreement, the section of the Agreement entitled 'Limitation of Liability' shall apply as between Controller and HubSpot, Inc., and in such respect any references to 'HubSpot', 'we', 'us' or 'our' shall include both HubSpot, Inc. and the HubSpot entity that is a party to the Agreement.

The legal entity agreeing to this DPA as Controller represents that it is authorized to agree to and enter into this DPA for, and is agreeing to this DPA solely on behalf of, the Controller.

**EXECUTED BY THE PARTIES AUTHORIZED REPRESENTATIVES:**

**HubSpot, Inc., by and on behalf of its affiliates, as applicable according to section 10 ('Parties to this DPA') above.**

Signature: 

Name: John P. Kelleher

Title: General Counsel

Controller: \_\_\_\_\_

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## **EXHIBIT 1**

### **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 Customer, as defined in the HubSpot Customer Terms of Service (the “data exporter”)**

And

**HubSpot Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141 (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 (j), 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 or 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.

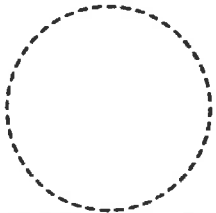
**On behalf of the data exporter:**

Name (written out in full): ...

Position: ...

Address: ...

Other information necessary in order for the contract to be binding (if any):

	Signature ...
---	---------------

**On behalf of the data importer:**

Name (written out in full): John Patrick Kelleher

Position: General Counsel

Address: 25 First Street, Cambridge, MA 02141 U.S.A.

Other information necessary in order for the contract to be binding (if any):

	Signature ... 
--	--

## **APPENDIX 1 to the Standard Contractual Clauses**

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

### **A. Data exporter**

The data exporter is the Customer, as defined in the HubSpot Customer Terms of Service ("**Agreement**").

### **B. Data importer**

The data importer is HubSpot, Inc., a global provider of inbound marketing and sales software.

### **C. Data subjects**

Categories of data subjects set out under Section 2 of the Data Processing Agreement to which the Clauses are attached.

### **D. Categories of data**

Categories of personal data set out under Section 2 of the Data Processing Agreement to which the Clauses are attached.

### **E. Special categories of data (if appropriate)**

The parties do not anticipate the transfer of special categories of data.

### **F. Processing operations**

The processing activities set out under Section 2 of the Data Processing Agreement to which the Clauses are attached:

DATA EXPORTER

Name: ...

Authorised Signature ...

DATA IMPORTER

Name: John P. Kelleher, General Counsel

Authorised Signature ...



## **Appendix 2 to the Standard Contractual Clauses**

This Appendix forms part of the Clauses.

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

HubSpot currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, HubSpot may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

### **a) Access Control**

#### **i) Preventing Unauthorized Product Access**

**Outsourced processing:** HubSpot hosts its Service with outsourced cloud infrastructure providers. Additionally, HubSpot maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. HubSpot relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

**Physical and environmental security:** HubSpot hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

**Authentication:** HubSpot implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

**Authorization:** Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of HubSpot's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

**Application Programming Interface (API) access:** Public product APIs may be accessed using an API key or through OAuth authorization.

#### **ii) Preventing Unauthorized Product Use**

HubSpot implements industry standard access controls and detection capabilities for the internal networks that support its products.

**Access controls:** Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

**Intrusion detection and prevention:** HubSpot implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

**Static code analysis:** Security reviews of code stored in HubSpot's source code repositories is performed, checking for coding best practices and identifiable software flaws.

**Penetration testing:** HubSpot maintains relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

**Bug bounty:** A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. HubSpot implemented a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

### iii) Limitations of Privilege & Authorization Requirements

**Product access:** A subset of HubSpot's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

**Background checks:** All HubSpot employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

## **b) Transmission Control**

**In-transit:** HubSpot makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the HubSpot products. HubSpot's HTTPS implementation uses industry standard algorithms and certificates.

**At-rest:** HubSpot stores user passwords following policies that follow industry standard practices for security. HubSpot has implemented technologies to ensure that stored data is encrypted at rest.

## **c) Input Control**

**Detection:** HubSpot designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. HubSpot personnel, including security, operations, and support personnel, are responsive to known incidents.

**Response and tracking:** HubSpot maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, HubSpot will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

**Communication:** If HubSpot becomes aware of unlawful access to Customer data stored within its products, HubSpot will: 1) notify the affected Customers of the incident; 2) provide a description of the steps HubSpot is taking to resolve the incident; and 3) provide status updates to the Customer contact, as HubSpot deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form HubSpot selects, which may include via email or telephone.

## **d) Availability Control**

**Infrastructure availability:** The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

**Fault tolerance:** Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

**Online replicas and backups:** Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases

are backed up and maintained using at least industry standard methods.

HubSpot's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists HubSpot operations in maintaining and updating the product applications and backend while limiting downtime.

**DATA EXPORTER**

Name: ...

Authorised Signature ...

**DATA IMPORTER**

Name: John Kelleher, General Counsel

Authorised Signature ...

