GDPR AND CCPA DATA PROCESSING ADDENDUM – ELASTIC CLOUD SERVICES

This Data Processing Addendum ("**Addendum**") forms part of the agreement between Customer (as defined below) and Elastic (as defined below) for Elastic Cloud Services (collectively the "**Agreemen**t"). For the purposes of this Addendum, "**Elastic**" means the entity identified as "Elastic" on the Order Form or in the applicable Agreement (if no Order Form is applicable) and "**Customer**" means the entity or individual identified as "Customer" on the Order Form or the entity or individual identified in the applicable Agreement as registering to use the Elastic Cloud Service(s) (if no Order Form is applicable).

This Addendum regulates the Processing of Personal Data for the Purposes (as described in Appendix 1 to Annex 1) in connection with the provision of one or more Elastic Cloud Services contemplated by the Agreement (the "**Services**"). The terms used in this Addendum have the meaning set forth in this Addendum. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Except as modified below, the terms of Agreement remain in full force and effect. Annex 1 (including Appendices 1 and 2 thereto) form an integral part of this Addendum.

The Parties agree that the terms and conditions set out below are added as an Addendum to the Agreement.

This Addendum and its provisions shall take effect on the Effective Date.

1. Definitions. The following terms have the meanings set out below for this Addendum:

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

   (b) "**Authorized Affiliate**" means any of Customer Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement.

   (c) "**Controller**" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

   (d) "**Data Protection Directive**" means the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

   (e) "**Data Protection Legislation**" means GDPR and the California Consumer Privacy Act of 2018 (CCPA).

   (f) "**Data Subject**" means any natural person whose Personal Data are Processed in the context of this Addendum.

   (g) "**Effective Date**" means the date of execution of this Addendum by Elastic and Customer.

   (h) "**Europe**" or "**European**" means the European Economic Area, Switzerland and Monaco.

   (i) "**GDPR**" or "**General Data Protection Regulation**" means 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.

   (j) "**Personal Data**" means (i) any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person and, for the purposes of this Addendum, specifically means (a) such information defined in sub clause (i) as is set forth under the descriptions "Data Subject" and "Categories of Personal Data" on Appendix 1 to Annex 1, and (b) information that meets the definition of "personal information" as set forth in the CCPA.

   (k) "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed.

   (l) "**Processor**" means the entity which Processes Personal Data on behalf of a Controller.

   (m) "**Processing of Personal Data**" (or "**Processing/Process**") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

   (n) "**Sub-Processor**" means the entity engaged by the Processor (including any Elastic Affiliate) or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

2. Roles of the Parties. In the context of the Agreement, the Parties agree that:

   (a) Customer acts as a Controller or Processor.

Where Customer is a Controller with regard to Personal Data, Customer appoints Elastic as Processor and where Customer is a Processor with regard to Personal Data, Customer appoints Elastic as a Sub-Processor, in each case, for the Processing of Personal Data identified on Appendix 1 to Annex 1 for the purpose of providing the Services specified in the Agreement and the applicable Order Form. In those contexts, Customer determines the purposes of the Processing of Personal Data that are disclosed to and/or collected by Elastic and Elastic will Process Personal Data only to carry out its obligations under the Agreement as implemented and on Customer's written instructions, where such instructions are consistent with the terms of the Agreement and the applicable Order Form. Except as set forth in this Addendum, Elastic shall not sell (as defined in the CCPA), share, transfer, transmit, disclose or otherwise provide access to or make available any Personal Data to any third party unless Customer has authorized Elastic to do so in writing.

3. Elastic's obligations. Elastic agrees it will:

(a) Immediately inform Customer, in writing, of any public authority of whatever jurisdiction requesting disclosure of or information about the Personal Data that are Processed by Elastic for and on behalf of Customer.

(b) Notify Customer when any law or legal requirement prevents Elastic (1) from fulfilling its obligations under this Agreement and have a substantial adverse effect on the guarantees provided by this Agreement, and (2) from complying with the instructions received from Customer via this Agreement, except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. In the context of (1) or (2), Customer is entitled to suspend the Processing of Personal Data to/by Elastic, and to terminate any further Personal Data Processing and/or terminate this Agreement, if doing so is required to comply with the Data Protection Legislation.

(c) To the extent required under Data Protection Legislation, keep internal records of Processing of Personal Data on behalf of Customer, containing at the minimum (i) the name and contact details of Elastic, and where applicable Elastic's representative and data protection officer; (ii) the categories of Personal Data Processed on behalf of Customer (to the extent provided by Customer to Elastic); (iii) where applicable, transfers of Personal Data outside of Europe; and (iv) a general description of the technical and organizational security measures listed in Appendix 2 to Annex 1.

(d) Immediately inform Customer in writing of and assist Customer with any requests to exercise the rights provided by the Data Protection Legislation with respect to Personal Data (e.g., access, modify, use or delete Personal Data, restrict the Processing, object to automated individual decision-making, and data portability) received from Customer or from Data Subjects in the context of the Services. Elastic will use commercially reasonable efforts to provide a copy of any such requests and that it shall respond to such requests only in accordance with Customer's prior written authorization and instructions. Elastic will assist Customer in fulfilling its obligations to respond to individuals' requests to exercise their rights in accordance with the Data Protection Legislation.

(e) Cooperate with Customer to fulfil Customer's own obligations under the Data Protection Legislation, including by assisting and cooperating with Customer in the conduct of data protection impact assessments and prior consultations with supervisory authorities.

(f) Upon termination of the Agreement or to comply with deletion requests or requests to return Personal Data, comply with Customer's request to delete, or return all the Personal Data to Customer, and delete existing copies unless applicable law prevents it from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case Elastic will protect the confidentiality of the Personal Data, will not actively Process the Personal Data anymore, and will continue to comply with this Addendum).

(g) Promptly inform the Customer if, in Elastic's opinion, an instruction infringes the Data Protection Legislation or other European Union or Member State laws.

4. Security of the Processing, Confidentiality, and Personal Data Breach Notification. Elastic agrees that it will:

(a) Maintain a comprehensive written information security program that complies with the Appendix 2 to Annex 1 of this Addendum and with the GDPR, including appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In assessing the appropriate level of security, Elastic shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

(b) Take steps to ensure that any person acting under its authority who has access to Personal Data is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only Processes Personal Data in accordance with Customer's documented instructions consistent with the terms of the Agreement and/or Order Form.

(c) Inform Customer in writing, without undue delay, after having become aware of a Personal Data Breach. Elastic will assist Customer in complying with its own obligations under the GDPR to notify of a Personal Data Breach as required under GDPR. Elastic will document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial actions taken.

5. International Data Transfers. With regard to Personal Data subject to GDPR, Elastic agrees that:

(a) It will not transfer Personal Data outside of Europe unless the Commission has determined that the country or territory to which such Personal Data provides adequate protection under Article 45 of GDPR without the explicit written consent of Customer. Customer agrees that Elastic may transfer or store Personal Data Processed on behalf of Customer outside of Europe or such other approved country or territory as necessary to perform Services on behalf of Customer. By signing this Addendum, the Parties conclude the Standard Contractual Clauses attached as Annex 1. The Elastic entity signing this Addendum executes the Standard Contractual Clauses on its own behalf and on behalf of its Affiliates and Customer executes the Standard Contractual Clauses on its own behalf and on behalf of its Authorized Affiliates. The Standard Contractual Clauses will apply to Personal Data Processed by Elastic in the context of the Services that are transferred outside of Europe or such other approved country or territory either directly or via an onward transfer. For the purposes of the Standard Contractual Clauses and this Section 5.1, the Customer and/or any Authorized Affiliate to which the Standard Contractual Clauses applies shall be deemed the "data exporter(s)". For the avoidance of doubt, where Customer has selected a data center located in Europe to host an Elastic Cloud Service, Elastic will not replicate or move Customer Personal Data to a data center located outside of Europe.

(b) The supervisory authority of Customer has the right to conduct an audit of Elastic and any Sub-Processor engaged by Elastic with regard to the Personal Data transferred to the United States, which has the same scope and is subject to the same conditions as would apply to an audit of Customer under the GDPR.

6. Elastic's Sub-Processing. With regard to Personal Data subject to the GDPR, Customer gives a general authorization to Elastic to engage Elastic Affiliates as internal Sub-Processors and to engage third parties as external Sub-Processors, in each case, in the context of the

Services and under the conditions set forth below and Elastic agrees that when sub-contracting the Processing of Personal Data in the context of the Services, it will:

(a) Require its internal and external Sub-Processors, via a written agreement, to comply with the Data Protection Legislation and with substantially the same obligations as are imposed on Elastic by this Addendum.

(b) Remain liable to the Customer for the performance of its Sub-Processors' obligations.

(c) Maintain a list of external Sub-Processors at https://www.elastic.co/agreements/cloud_services/external_subprocessors. and a list of internal Sub-Processors (Elastic Affiliates) at https://www.elastic.co/agreements/cloud_services/internal_subprocessors.

(d) Elastic will notify the Customer of any addition or replacement of a Sub-Processor in a timely fashion so as to give the Customer an opportunity to object to the change before the Personal Data is communicated to the new Sub-Processor. Notification of any such new Sub-Processor may be provided via the administrative console for the applicable Cloud Service. Customer may object to Elastic's use of a new Sub-Processor by notifying Elastic promptly in writing within ten (10) days after receipt of Elastic's notice in accordance with the notice provisions of the Agreement. If Customer does not object within this time period his acceptance of the new Sub-Processor shall be deemed granted. If Customer has objected to a new Sub-Processor, Elastic will use reasonable efforts to make available to Customer a change in the respective Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor. If such change is not possible with reasonable efforts within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate in writing the applicable Order Form with respect only to those Services which cannot be provided by Elastic without the use of the new Sub-processor Elastic shall promptly refund any pre-paid unused fees with respect to the terminated Services.

7. Data Protection Audit. Upon prior written request by Customer, to the extent required under the Data Protection Legislation, Elastic agrees to cooperate and within reasonable time provide Customer with: (a) a summary of any required audit reports demonstrating Elastic's compliance with EU Data Protection obligations under this Addendum (without any confidential or commercially sensitive information); and (b) confirmation that such audit has not revealed any material vulnerability in Elastic's systems, or to the extent that any such vulnerability was detected, that Elastic has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with Data Protection Legislation or reveal some material issues, subject to the strictest confidentiality obligations, Elastic allows Customer to request an audit of Elastic's data protection compliance program by external independent auditors, which are jointly selected by the Parties, at Customer's sole expense. The Parties will mutually agree upon the scope, timing, and duration of the audit. Elastic will make available to Customer the result of the audit of its data protection compliance program.

8. Applicable Law and Jurisdiction. This Addendum shall be governed in accordance with the governing law, jurisdiction and venue provisions of the Agreement, except as otherwise set forth in the Standard Contractual Clauses or where mandatory law provides for the courts at another location to have jurisdiction.

9. Authorized Affiliates. The parties acknowledge and agree that, by executing the Agreement, Customer enters into this Addendum on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate Addendum between Elastic and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement but is only a party to this Addendum. Customer shall remain responsible for coordinating all communication with Elastic under this Addendum and be entitled to make and receive any communication in relation to this Addendum on behalf of its Authorized Affiliates. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

ANNEX 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 entity identified as “Customer” in the Addendum, which is deemed the **data exporter**

And

The entity identified as “Elastic” in the Addendum, which is deemed 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.

APPENDIX 1 TO ANNEX 1 – STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Data controller (Customer)
Customer administers Elastic Cloud Service(s) on behalf of itself and its Authorized Affiliates. Customer and its Authorized Affiliates may elect to transfer personal data of data subjects (as described below) in connection with Customer's or its Authorized Affiliates' use of Elastic Cloud software-as-a-service product(s) (see https://www.elastic.co/cloud), hereinafter referred to as "Elastic Cloud Service(s)") and/or to enable Elastic to perform diagnostic measures in connection with fulfilling its Services obligations with regard to the Customer's or its Authorized Affiliates' use of Elastic Cloud Service(s), in each case, as set forth in the Agreement. References in this Appendix 1 to Customer's use of Elastic Cloud Service(s) shall also include use of Elastic Cloud Service(s) by Authorized Affiliates.

Data processor (Elastic)
Elastic makes Elastic Cloud Service(s)available on a software-as-a-service basis and provides Services with regard to Customer's use of Elastic Cloud Service(s), in each case, as set forth in the Agreement.

Data subjects
Personal data transferred to Elastic Cloud Service(s) and/or the Services may concern the following categories of data subjects: individuals whose personal data Customer elects to transfer to Elastic for Processing by Elastic Cloud Service(s) or for the performance of diagnostic measures by Elastic in connection with fulfilling its Services obligations with regard to the Customer's use of Elastic Cloud Service(s), in each case, as set forth in the Agreement.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Use of Elastic Cloud Service(s) by Customer. Personal data relating to individuals that Customer elects to transfer to an Elastic Cloud Service(s) for Processing by such Elastic Cloud Service.

Diagnostics. Personal data relating to individuals that may be contained in data files that have been recorded at a particular time during a computing process and are then provided to Elastic's support engineers in connection with troubleshooting an error or performance issue.

Special categories of data (if appropriate)

No Sensitive personal data (as defined by GDPR) is transferred.

Processing operations (or purposes)

Personal data that Customer elects to transfer to an Elastic Cloud Service is stored in and processed by such Elastic Cloud Service and/or provided in connection with Elastic support engineers troubleshooting an error or performance issue.

APPENDIX 2

APPENDIX 2.1 TO ANNEX 1 – STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Elasticsearch Service

Description of the technical and organisational security measures implemented by the data processor:

The data processor will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of personal data provided by the data exporter in fulfilment of the Services, including the following:

1. Physical access control

Sub-Processors hosting the Services are reviewed to determine whether they have appropriate security measures implemented to control physical access to the systems used to deliver the Services (see description of security measures in Annex 1).

2. Logical access control

Internal access by data processor employees to Customer Support Portal and remote access to Elasticsearch Service by data processor employees requires two-factor authentication with named user accounts and complex passwords with a minimum length.

3. Data access control

Technical and organizational measures are implemented to ensure that persons entitled to access a data processing system gain access only to personal data in accordance with their differentiated access rights (profiles, roles, transactions and objects), and that personal data cannot be read, copied, modified or deleted without authorization.

4. Disclosure control

Technical and organizational measures are implemented to ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport, or storage, including encryption in transit for access to support systems.

5. Availability control

Customer Support Portal and Elasticsearch Service (if Customer elects “high availability” implementation) are each hosted by a Sub-Processor that provides “high availability” so that personal data are protected against accidental destruction or loss (physical/logical).

7. Separation control

Technical and organizational measures are implemented to ensure that personal data uploaded by Customer for processing in Elasticsearch Service is processed separately.

APPENDIX 2.2 TO ANNEX 1 – STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Site Search Service and/or App Search Service

Description of the technical and organisational security measures implemented by the data processor:

The data processor will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of personal data provided by the data exporter in fulfilment of the Services, including the following:

1. Physical access control

Sub-Processors hosting the Services are reviewed to determine whether they have appropriate security measures implemented to control physical access to the systems used to deliver the Services.

2. Logical access control

Internal access by data processor employees to the Site Search Service and/or App Search Service Dashboard and remote access to Site Search Service and/or App Search Service Production environment by data processor employees requires two-factor authentication with named user accounts and complex passwords with a minimum length. Role-based access controls implemented on all employee-facing components of Site Search Service and/or App Search Service Production environment.

3. Data access control

Technical and organizational measures are implemented to ensure that persons entitled to access a data processing system gain access only to personal data in accordance with their differentiated access rights (profiles, roles, transactions and objects), and that personal data cannot be read, copied, modified or deleted without authorization.

4. Disclosure control

Technical and organizational measures are implemented to ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport, or storage, including encryption in transit for access to support systems.

5. Availability control

Site Search Service and/or App Search Service Dashboard and Site Search Service and/or App Search Service API are deployed in a highly-available manner with redundancy on all layers to protect against accidental destruction or loss (physical/logical). Full backups of personal data are performed on a daily basis and backups are automatically tested to ensure consistency.

7. Separation control

Technical (logical) and organizational measures are implemented to ensure that personal data uploaded by Customer for processing using Site Search Service and/or App Search Service APIs is processed separately from other customers. Physical separation controls could be applied to the data from specific customers (subject to custom agreements).