Elastic – Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the agreement between Customer (as defined below) and Elastic (as defined below) for Elastic Cloud Services (collectively, the "**Agreement**"). For the purposes of this DPA, "**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 DPA describes the commitments of Elastic and the Customer (each a "**party**" and together, the "**parties**") concerning the processing of Personal Data in connection with the provision of one or more Elastic Cloud Services (the "**Cloud Services**") contemplated by the applicable Agreement.

The terms used in this DPA have the meaning set forth in this DPA. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement.

The parties agree as follows:

1.   **Definitions**. The following capitalized terms, when used in this DPA, will have the corresponding meanings provided below:

1.1   **"Applicable Data Protection Laws"** means European Data Protection Laws and the California Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq ("**CCPA**"); as may be amended, superseded or replaced.

1.2   **"Customer Personal Data"** means any Personal Data processed by Elastic on behalf of Customer as a service provider or processor (as applicable) in connection with the Cloud Services, as more particularly described in Annex A of this DPA**.**

1.3   "**EEA**" means the countries that are parties to the agreement on the European Economic Area and the United Kingdom and Switzerland.

1.4   **"European Data Protection Laws"** means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ("**e-Privacy Directive**"); (iii) any applicable national implementations of (i) and (ii); (iv) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance; and (v) in respect of the United Kingdom, the Data Protection Act 2018 and any applicable national legislation that replaces or converts in domestic law the GDPR, e-Privacy Directive or any other law relating to data and privacy as a consequence of the UK leaving the European Union; in each case as may be amended, superseded or replaced.

1.5   "**Standard Contractual Clauses**" means the standard contractual clauses for processors as approved by the European Commission pursuant to its decision C(2010)593 of 5 February 2010 and sometimes referred to as Standard Contractual Clauses.

1.6   **"Personal Data"** means any information that relates to an identified or identifiable natural person and which is protected as "personal data", "personal information" or "personally identifiable information" under Applicable Data Protection Laws.

1.7   "**Security Breach**" has the meaning set forth in the applicable Information Security Addendum to the Agreement.

1.8   **"Sub-processor"** means any processor engaged by Elastic or its Affiliates to assist in fulfilling its obligations with respect to providing the Cloud Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Elastic Affiliates.

1.9   The terms **"controller", "processor"** and "**processing**" shall have the meanings given to them in the GDPR, and **"process", "processes"** and **"processed"** shall be interpreted accordingly; and the terms **"business", "service provider"** and **"sell"** shall have the meanings given to them in the CCPA**.**

2.   Role and Scope of Processing

2.1   **Scope.** This DPA applies to the extent that Elastic processes as a processor or service provider (as applicable) any Customer Personal Data.

2.2   **Role of the Parties.** The parties acknowledge and agree that Customer is a business or the controller (as applicable) with respect to the processing of Customer Personal Data, and Elastic shall process Customer Personal Data only as a processor or service provider (as applicable) on behalf of Customer (notwithstanding that Customer may be a service provider or a processor acting on behalf of its own customers and in such case Elastic shall process Customer Personal Data as a service provider or a sub-processor acting on behalf of Customer), as further described in Annex A of this DPA. Any processing by either party of Customer Personal Data under or in connection with the Cloud Services shall be performed in accordance with Applicable Data Protection Laws.

2.3   **Elastic Processing of Personal Data.** Elastic agrees that it shall process Customer Personal Data only for the purposes described in the Agreement and in accordance with Customer's documented lawful instructions. The parties agree that the Agreement and applicable Order Form (including this DPA) sets out the Customer's complete and final instructions to Elastic in relation to the processing of Customer Personal Data. Without prejudice to Section 2.4 (Customer Responsibilities), Elastic shall notify Customer in writing, unless prohibited from doing so under Applicable Data Protection Laws, if it becomes aware or believes that any data processing instructions from Customer violates Applicable Data Protection Laws.

2.4   **Customer Responsibilities.** Customer is responsible for the lawfulness of Customer Personal Data processing under or in connection with a Cloud Service. Customer shall (i) have provided, and will continue to provide all notices and have obtained, and will continue to obtain, all consents, permissions and rights necessary under Applicable Data Protection Laws for Elastic to lawfully process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA); (ii) have complied with all Applicable Data Protection Laws applicable to the collection and provision of Customer Personal Data to Elastic and its Sub-processors of such Customer Personal Data; and (iii) ensure its processing instructions comply with applicable laws (including Applicable Data Protection Laws).

3.   Subprocessing

3.1   **Authorized Sub-processors.** Customer acknowledges and agrees that Elastic may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Sub-processors currently engaged by Elastic and authorized by Customer are available for external Sub-processors here (https://www.elastic.co/agreements/cloud_services/external_subprocessors) and for internal Sub-processors here (https://www.elastic.co/agreements/cloud_services/internal_subprocessors). Elastic shall notify Customer if it changes its Sub-processors in advance to any such changes via the administrative console for the applicable Cloud Service.

4.   Security and Audits

4.1   **Elastic Security Standards**. Elastic shall implement and maintain the appropriate technical and organizational security measures defined in the Elastic Security Standards (as defined in the Agreement) to protect Customer Personal Data from Security Breach (as defined in

1

the Elastic Security Standards) and to preserve the security and confidentiality of the Customer Personal Data. Such measures will include, at a minimum, those measures described in the Elastic Security Standards specific to the Cloud Services. Elastic shall ensure that any person who is authorized by Elastic to process Customer Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.2 **Customer Security Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer shall implement and maintain appropriate technical and organizational security measures designed to protect Personal Data from Security Breaches and to preserve the security and confidentiality of Customer Personal Data while in its dominion and control.

4.3 **Security Breach Response**. Upon becoming aware of a Security Breach, Elastic shall notify Customer in accordance with Section 3 of the Elastic Security Standards.

4.4 **Security Audits.** Elastic shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its processing of Customer Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Elastic's compliance with this DPA, provided that Customer shall not exercise this right more than once in any 12 month rolling period. Notwithstanding the foregoing, Customer may also exercise such audit right in the event Customer is expressly requested or required to provide this information to a data protection authority on another reasonably similar basis.

5. International Transfers

5.1 **Processing locations.** Customer acknowledges and agrees that Elastic may transfer and process Customer Personal Data to and in the United States and anywhere else in the world where Elastic, its Affiliates or its Sub-processors maintain data processing operations. Elastic shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this DPA.

6. Deletion of Customer Personal Data

6.1 Upon termination or expiry of a Cloud Services Subscription, Elastic shall delete all Customer Personal Data (including copies) in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent Elastic is required by applicable law to retain some or all of the Customer Personal Data.

7. Rights of Individuals and Cooperation

7.1 **Data Subject Requests.** To the extent that Customer is unable to independently access the relevant Customer Personal Data within the Cloud Services, Elastic shall, taking into account the nature of the processing, provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Personal Data under the Agreement. In the event that any such request is made to Elastic directly, Elastic shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Elastic is required to respond to such a request, Elastic shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

7.2 **Subpoenas and Court Orders**. If a law enforcement agency sends Elastic a demand for Customer Personal Data (for example, through a subpoena or court order), Elastic shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Elastic is legally prohibited from doing so.

8. Jurisdiction Specific Terms

8.1 **Europe.** To the extent the Customer Personal Data is subject to European Data Protection Laws, the following terms shall apply in addition to the terms in the remainder of this DPA:

(a) <u>Sub-processor Obligations.</u> Elastic shall: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect personal data to the standard required by applicable European Data Protection Law and this DPA; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Elastic to breach any of its obligations under this DPA.

(b) <u>Objections to Sub-processors.</u> Customer may object in writing to Elastic's appointment of a new Sub-processor by notifying Elastic promptly in writing within ten (10) calendar days of receipt of Elastic notice in accordance with Section 3.1 above. Such notice shall explain the reasonable grounds for the objection and the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If no such resolution can be reached, Elastic will, at its sole discretion, either not appoint Sub-processor, or permit Customer to suspend or terminate the affected Cloud Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

(c) <u>Standard Contractual Clauses</u>**.** Elastic agrees to abide by and process Customer Personal Data in compliance with the Standard Contractual Clauses, which are attached hereto as Exhibit A and form an integral part of this DPA. For the purposes of the descriptions in the Standard Contractual Clauses: (i) Elastic agrees that it is a "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be an entity located outside the EEA); (ii) Annex A of this DPA shall replace Appendix 1 of the Standard Contractual Clauses; (iii) the Elastic Security Standards will replace Appendix 2 of the Standard Contractual Clauses; and (iv) Annex B shall form Appendix 3 of the Standard Contractual Clauses. It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

(d) <u>Transfers after Brexit</u>: In the event that European Union law ceases to apply to the United Kingdom upon the United Kingdom's withdrawal from the European Union then to the extent Elastic processes (or causes to be processed) any Customer Personal Data originating from the EEA in the United Kingdom, Elastic agrees to abide by and process such Customer Personal Data in compliance with the Standard Contractual Clauses (which shall be incorporated in accordance with Section 8.1 (c)), until such time as the European Commission determines the United Kingdom provides an adequate level of protection for personal data (a "**UK Adequacy Decision**") (or makes a determination as to other safeguards), from which date (i) the parties will rely on the UK Adequacy Decision (or other safeguards) in respect of such processing, and (ii) the parties will put in place all necessary documentation, if any, as required by European Data Protection Laws in order to formalise their reliance on the UK Adequacy Decision (or other safeguards) to enable the lawful transfer of personal data.

(e) <u>Data Protection Impact Assessment.</u> To the extent Elastic is required under applicable European Data Protection Law, Elastic shall provide reasonably requested information regarding Elastic's processing of Customer Personal Data under the Agreement to enable the Customer to carry out data protection impact assessments or prior consultations with supervisory authorities as required by law.

8.2   **California.** To the extent the Customer Personal Data is subject to the CCPA, the parties agrees that Customer is a business and that it appoints Elastic as its service provider to process Customer Personal Data as permitted under the Agreement (including this DPA) and the CCPA, or for purposes otherwise agreed in writing (the "**Permitted Purposes**"). Customer and Elastic agree that: (a) Elastic shall not retain, use or disclose personal information for any purpose other than the Permitted Purposes; (b) Customer Personal Data was not sold to Elastic and Elastic shall not "sell" personal information (as defined by the CCPA); (c) Elastic shall not retain, use or disclose personal information outside of the direct business relationship between Customer and Elastic; and (d) Elastic may de-identify or aggregate personal information in the course of providing the Cloud Services. Elastic certifies that it understands the restrictions set out in this Section 8.2 and will comply with them.

9.   Miscellaneous

9.1   Except for the changes made by this DPA as applicable to the Cloud Services, the Agreement remains unchanged and in full force and effect.

9.2   This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by European Data Protection Laws.

v090120.1 – Elastic Cloud Services Data Processing Addendum – ES ALL

Exhibit A

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.

Annex A
Data Processing Description

This Annex A forms part of this DPA and describes the processing that the processor will perform on behalf of the controller.

Data controller (Customer)

Customer administers Cloud Service(s) on behalf of itself and its Affiliates. Customer and its Affiliates may elect to transfer personal data of data subjects (as described below) in connection with Customer's or its Affiliates' use the Cloud Services, as set forth in the Agreement. References in this Annex A to Customer's use of the Cloud Services shall also include use of such Cloud Services by Customer Affiliates.

Data processor (Elastic)

Elastic provides the Cloud Services as set forth in the Agreement.

Duration

The duration of the processing under this DPA is until the termination of the Cloud Service in accordance with its terms plus the period from the expiry of the Subscription Term until deletion of personal data by Elastic in accordance with the terms of the Agreement.

Categories of data

The Customer Personal Data transferred concern the following categories of data (please specify):
- Use of the Cloud Services by Customer. Customer Personal Data that Customer elects to transfer to a Cloud Service for processing by such Cloud Service.
- Diagnostics. Customer Personal Data 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

The parties do not intend for any special category data to be processed under the Agreement.

Data subjects

Customer Personal Data transferred to the Cloud Services may concern the following categories of data subjects: individuals whose personal data or personal information Customer elects to transfer to Elastic for processing by the Cloud Service as set forth in the Agreement.

Processing operations

Customer Personal Data that Customer elects to transfer to a Cloud Service processed by such Cloud Service as set forth in the Agreement.

Annex B

This Appendix forms part of the Standard Contractual Clauses. All defined terms used in this Appendix 3 shall have the meaning given to it in the Standard Contractual Clauses unless otherwise defined in this Appendix.

Appendix 3 to the Standard Contractual Clauses

This Appendix sets out the parties' interpretation of their respective obligations under specific clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses. For the purposes of this Appendix, "**DPA**" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated and "**Agreement**" shall have the meaning given to it in this DPA.

Clause 4(h) and 8: Disclosure of these Clauses

1.   Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1.   The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2.   The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.

3.   If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").

4.   If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1.   Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 4 (Security and Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1.   The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2.   The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3.   Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1.   Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1.   The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.

2.   Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 8.1 of the DPA.