**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 Offerings (as defined below) (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 Elastic's Cloud Services, Support Services and/or Consulting Services (collectively, the "**Elastic Offerings**") (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 Offerings 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Laws and the California Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq ("**CCPA**"); as may be amended, superseded or replaced.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 Elastic Offerings, as more particularly described in Annex I of this DPA**.**

1.3 "**Elastic Security Standards**" mean Elastic's then-current security standards for the processing of Content as set forth at https://www.elastic.co/pdf/elastic-information-security-addendum-consolidated-v030121.0.pdf.

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

1.5 **"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, as amended by Directive 2009/136/EC ("**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 ("**UK**"), 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; in each case as may be amended, superseded or replaced.

1.6 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses as adopted by the EU Commission by means of the Implementing Decision EU 2021/914 of June 4, 2021.

1.7 **"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.

1.8 "**Security Breach**" has the meaning set forth in the Elastic Security Standards.

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

1.10 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 I of this DPA. Any processing by either party of Customer Personal Data under or in connection with the Elastic Offerings 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 the Elastic Offerings. 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 as set forth at https://www.elastic.co/agreements/external_subprocessors and for internal Sub-processors as set forth at https://www.elastic.co/agreements/internal_subprocessors. Elastic shall notify Customer if it changes its Sub-processors in advance to any such changes for the applicable Elastic Offering(s). Elastic's notification shall be through email communications to Customer and Customer must sign-up to receive the email notifications through RSS web feed links. To sign-up, use the weblinks set forth in this Section 3.1.

## 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 to protect Customer Personal Data from Security Breach 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 Elastic Offerings. 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 the applicable Elastic Offering, or earlier in accordance with the applicable data retention policy for the Elastic Offering, 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 Elastic Offerings, 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 **EEA and UK.** 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) Sub-processor Obligations. 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) Objections to Sub-processors. 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 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 Elastic Offerings 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) Data Protection Impact Assessment. 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 assist the Customer to carry out data protection impact assessments or prior consultations with supervisory authorities as required by law.

8.2 **Personal Data Transfers outside of the EEA.** 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 I shall serve as Annex I of the Standard Contractual Clauses; (iii) the Elastic Security Standards will serve as Annex II of the Standard Contractual Clauses; and (iv) Annex III shall form Annex III 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.

8.3 **Personal Data Transfers outside of the UK**. Elastic agrees to abide by and process Customer Personal Data in compliance with the clauses annexed to 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, which are hereby incorporated and completed as follows: the governing law in Clause 9 and Clause 11.3 is the law of England and Wales, and Appendix 1 and Appendix 2 and Appendix 3 are Annexes I,II and III to this DPA respectively. In addition, the following changes apply: (i) references to Data Protection Law are replaced with references to applicable UK data protection law, (ii) references to the EU or Member States are replaced with references to the UK, and (iii) references to EU authorities are replaced with references to the competent UK authority. In the event the competent UK authorities adopt the Standard

Contractual Clauses, effective upon such adoption, the transfer of Customer Personal Data shall be governed by the Standard Contractual Clauses (as referenced in Exhibit A hereto) to the extent permitted under applicable UK law.

8.4 **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 Elastic Offerings. 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 Elastic Offerings, 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.

**Exhibit A to the DPA**

## Standard Contractual Clauses
(MODULE TWO – CONTROLLER TO PROCESSOR)

### SECTION I

### Clause 1
### Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

### Clause 2
### Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### Clause 3
### Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### Clause 4
### Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### Clause 5
### Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### Clause 6
### Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### Clause 7
### Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II – OBLIGATIONS OF THE PARTIES

### Clause 8
### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### 8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### 8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

#### 8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### 8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### 8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### Clause 9
### Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### Clause 10
### Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

### Clause 11
### Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

### Clause 12
### Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### Clause 13
### Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

### Clause 14
### Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## Clause 15
## Obligations of the data importer in case of access by public authorities

### 15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### 15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(c).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

## Clause 16
## Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### Clause 17
### Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

### Clause 18
### Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts**.**

## ANNEX I to Exhibit A

## Data Processing Description

### A. LIST OF PARTIES

**Data exporter(s):**

**1.** Name: Customer
Address: As stated in Customer's underlying Agreement or on Customer's Account
Contact person's name, position and contact details: The Contact information provided by Customer in its Account
Activities relevant to the data transferred under these Clauses: Customer administration, receipt and/or use of the Elastic Offering(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 of the Elastic Offerings, as set forth in the Agreement. References in this Annex I to Customer's use of the Elastic Offerings shall also include use of such Elastic Offering(s) by Customer Affiliates.
Role : Controller

**Data importer(s):**

**1.** Name: Elastic
Address: As described in Customer's Underlying Agreement or Order Form
Contact person's name, position and contact details: To the Legal Department as described in the Notice section of the underlying agreement.
Activities relevant to the data transferred under these Clauses: Elastic provides the Elastic Offerings as set forth in the Agreement.
Signature and date: As per the Effective date and signature per the Underlying Agreement.
Role (controller/processor): Processor

### B. DESCRIPTION OF TRANSFER

- **Categories of data subjects whose personal data is transferred**

Customer Personal Data transferred to Elastic may concern the following categories of data subjects: individuals whose personal data or personal information Customer elects to transfer to Elastic for processing for the provision, receipt and/or use of the applicable Elastic Offering(s) as set forth in the Agreement.

- **Categories of personal data transferred**

The Customer Personal Data transferred concern the following categories of data (please specify):
- <u>Use of the Elastic Offering by Customer</u>. Customer Personal Data that Customer elects to transfer to Elastic for processing for the provision of the applicable Elastic Offering.
<u>- Diagnostics</u>. 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.

- **Sensitive data transferred**

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

- **Frequency of the transfer**

For the duration of Customer's services purchased from Elastic.

- **Nature of the processing**

Customer Personal Data that Customer elects to transfer to Elastic to be processed for the provision, receipt and/or use of the applicable Elastic Offering as set forth in the Agreement.

- **Purpose(s) of the data transfer and further processing**

The operation, support, use or provisioning of the services as set out in the Agreement and compliance with applicable laws.

- **The period for which the personal data will be retained**

The duration of the processing under this DPA is until the termination or expiration of the applicable Elastic Offering(s) in accordance with its terms plus the period from the expiry of the applicable Elastic Offering(s) until deletion of personal data by Elastic in accordance with the terms of the Agreement.

### C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority of the Netherlands shall act as competent supervisory authority.

## Annex II to Exhibit A

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA: as described in the Elastic Security Standards (defined in the DPA) as set forth at https://www.elastic.co/pdf/elastic-information-security-addendum-consolidated-v030121.0.pdf.

## Annex III to the Standard Contractual Clauses

This Annex III 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 Annex, 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. In the event of a contradiction between this Annex III and the SCCs in Exhibit A, the provisions of the SCCs in Exhibit A shall prevail.

**Clauses 8.3 and 13: 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 8.3 or a supervisory authority pursuant to Clause 13.

**Clause 16: 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 8.9: Audit:**

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

**Clause 9(c): 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 12: 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.