# Supplier Data Processing Agreement

|  |  |
| --- | --- |
| \_\_ \_\_\_\_\_\_\_\_\_\_\_\_ 2018 |  |

Crowdin Inc., a legal entity incorporated under the laws of Delaware, USA at 8 The Green Dover, DE 19901, registration number 364861388, represented by \_\_\_\_\_\_\_, (the “**Supplier**”)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** a legal entity incorporated under the laws of \_\_\_\_\_\_\_\_\_\_ at \_\_\_\_\_\_\_\_\_\_\_\_, registration number \_\_\_\_\_\_\_\_\_\_, represented by \_\_\_\_\_\_\_, (the “**Customer**”)

hereinafter collectively referred to as the “**Parties**” have entered into this Supplier Data Processing Agreement (“**DPA**”) as a part of the Customer’s use of the Supplier’s Service under the Subscription and Support Agreement (the “Agreement”) on the following terms:

1. **Definitions.**

All capitalised used in this DPA will have the means given to them below:

**“Affiliate”** means any entity that directly or indirectly owns or controls, is owned or controlled by, or is under the common ownership or control with a party.

**“Applicable laws”** means (a) European Union or Member State laws with respect to any Personal Data in respect of which Supplier is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Personal Data in respect of which the Supplier is subject to any other Data Protection Laws;

**The terms, “Personal data”, “Special categories of data”, “Process/processing”, “Controller”, “Processor”, “Personal Data Breach”, “Sub-processor”, “Data subject” and “Supervisory authority”** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

“**Personal Data**” means any Personal Data within the meaning given to it in GDPR processed by Supplier (or a Sub-processor) on behalf of Customer pursuant to or in connection with the DPA and/or the Agreement.

**“Confidential Information”** any and all non-public information disclosed to the Receiving Party by the Disclosing Party, whether in the past, now or in the future, in any form or format whatsoever, whether tangible or intangible, including Intellectual Property Rights, whether or not subject to or protected by registered or unregistered copyright, patent, trademark, existing now or in the future, that relates to the Disclosing Party or their business, prospective business, finances, budgets, costs, marketing, contracts, suppliers, customers, employees, or investors; technical processes, computer software or programs (including source code and object code), trade secrets, know-how, inventions, applications, documentation, schematics, data, designs, drawings, works in progress, engineering, security reports and information, penetration test reports, formulae, or other test data; correspondence with governmental agencies or authorities; or the terms of any agreement negotiated or entered into between the Parties and the discussions, negotiations, and proposals related to any such negotiation or agreement, where the information is: (i) clearly and conspicuously marked as “confidential” or “proprietary” or with a similar designation; (ii) identified by the Disclosing Party as confidential and/or proprietary before, during, or promptly after presentation or communication; or (iii) disclosed in a manner in which the Disclosing Party reasonably communicated, or the Receiving Party should reasonably have understood, that the disclosure should be treated as confidential, whether or not the specific designation "confidential" or “proprietary” or any similar designation is used.

"**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

**“GDPR”** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

**Standard Contractual Clauses** means Appendix 1 attached to and forming part of this DPA pursuant to the European Commission Decision of 5 February 2010, amended as indicated (in square brackets and italics) in that Appendix 1 and under section [3.2.](#_Ref483203635) of this DPA.

**Third Country** means a country outside the European Economic Area.

**“Data exporter”** and **“Data importer”** are determined in Standard Contractual Clauses and for the purposes of this DPA mean Customer and Supplier respectively.

1. **Data Processing** 
   1. **Scope**: This DPA, including any attachments, exhibits or appendixes as applicable, form part of the Agreement or other written or electronic agreement between Customer and Supplier. This DPA reflects the Parties’ understanding with respect to the terms governing the processing of Personal Data provided to Supplier by the Customer under the Agreement.
   2. **Conflict of Meaning**. To the extent that there is any conflict between the terms of the Agreement and this DPA the terms if this DPA shall prevail. To the extent that there is any conflict between a term of Appendix 1 and any other term in this DPA, the meaning of the term in Appendix 1 shall prevail.
   3. **Data Processing** by the Supplier: Supplier will only process Personal Data in accordance with the with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and other applicable document(s); (ii) Processing initiated by Customer in their use of the Supplier’s Service; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement and the DPA.
   4. **Access or Use:** Supplier will not access or use Personal Data, except as necessary to provide the Services and only if requested and authorised by the Customer.
   5. **Controller and Processor:** Supplierwill at all times remain the Processor or a Sub-processor of Personal Data under the Agreement and DPA. Depending on the nature of services provided by the Supplier to the Customer the Customer will act as a Controller of Personal Data or as a Processor of Personal Data. The Customer will comply with its obligation as a Controller under the Data Protection Laws. Supplier will comply with its obligations as a Processor and/or Sub-processor under Data Protection Laws, the Agreement, this DPA, and any instructions that may be provided to Supplier by the Customer any time thereafter. Supplier will only process Personal Data as instructed under this DPA and will not process Personal Data for any other purpose.
   6. **Sub-processing:** Supplier / Supplier Affiliate to act as or appoint Sub-processors in accordance with section 8 of this DPA. If applicable, the Supplier shall ensure that each Sub-processor performs the obligations under this DPA, as if it were party to this DPA in place of Suppler.
2. **Application of Standard Contractual Clauses (Appendix 1, 2 and 3 as applicable).** 
   1. The Standard Contractual Clauses will apply to Personal Data that is processed by Supplier, either directly or by onward transfer, within the EEA or to any Third Country, unless replaced or amended by the Commission or an equivalent Competent Authority. In case of adoption of any equivalent contractual clauses and/or amending the existing Standard Contractual Clauses to reflect Data Protection Laws, the latter shall be applied to processing of Personal Data by the Supplier.
   2. The Supplier may substitute the Standard Contractual Clauses contained in Appendix 1 or add new standard contractual clauses adopted by the data protection authorities in appropriate way to address the requirements of any Data Protection Law.
3. **Term.** 
   1. This DPA will take effect on the effective date of the Agreement or date of final signature below, whichever is earlier

1. **Security obligations of the Supplier.**

* 1. Supplier and each Supplier Affiliate shall in relation to the Personal Data implement appropriate technical and organizational measures taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons as it is envisaged by Article 32 of the GDPR.
  2. Supplier has implemented adequate technical and organizational measures as specified in the Appendix 3 to this DPA to ensure a level of security appropriate to the nature of processing of Personal Data implied by the Agreement. All servers and public web-services with personal data are processed based on an HTTPS protocol using security certificates. The access to the sensitive personal data is protected either by firewalls or can be accessed only using cryptographic network protocol. The firewall security policies are managed solely by the Supplier.
  3. Supplier shall implement restrict access and use of Personal Data to those personnel and authorised representatives who have a need to process the Personal Data to fulfil Supplier’s obligations under the Agreement.
  4. Supplier shall ensure that the arrangement between on the one hand (a) Supplier, or (b) the relevant Supplier Affiliate, or (c) the relevant Sub-processor, is governed by a written contract including terms which offer at least the same level of protection for Personal Data as those set out in this DPA and meet the requirements of article 28(4) of the GDPR. If that arrangement involves a transfer he countries outside EEA, the Supplier shall ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Supplier, or (b) the relevant Supplier Affiliate, or (c) the relevant Sub-processor unless other safeguards for transfer are implemented pursuant to the requirements of GDPR.
  5. Customer confirms that all the technical and organizational measures taken by the Supplier to protect Personal Data are adequate and comply with the legislative requirements.

1. **Rights of Data Subjects and corresponding obligations of the Supplier**
   1. **Correction, Blocking and Deletion**. Supplier will rectify, erase or block the processing of Personal Data on the request of the Customer if such rectification, erasure or blocking are provided by law. Supplier may retain Personal Data to the extent required by applicable Data Protection Laws and only to the extent and for such period as required by applicable Data Protection Laws and provided that Supplier and each Supplier Affiliate or Sub-processor shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable Data Protection Laws requiring its storage and for no other purpose.
   2. **Data Subject Requests**. If Supplier receives a request from a Data Subject to access, correct, block, release or delete the Personal Data processed by the Supplier, or otherwise exercise their rights, Supplier will promptly, but not later than 10 working days after receipt, forward the request to the Customer, to the extent legally permitted. Supplier will cooperate and assist the Customer in relation to any request of a Data Subject’s request.
   3. The Supplier shall not disclose Personal Data to any Data Subject or to a third party other than at the request of the Customer or as provided for in this DPA.

1. **Personal Data Breach.** 
   1. Supplier must notify the Customer without undue delay in case of a security breach or data leakage or if Personal Data is lost, destroyed or becomes damaged, corrupted or unusable. The notification shall describe in clear and plain language the nature of the personal data breach and contain at least the name and contact details of the contact point where more information can be obtained, a description of the likely consequences of the personal data breach and a description of the measures taken or proposed to be taken by the Supplier to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
   2. Supplier shall co-operate with Customer and take such reasonable measures as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

1. **Affiliates and Sub-processors.** 
   1. The Customer agrees that some of Supplier’s obligation under the Agreement may be performed by the Supplier Affiliates provided that the sub-contractor's contract is on terms which are substantially the same as those set out in this DPA.
   2. The Supplier may only authorize a third party (sub-processor) to process the Personal Data:
      1. provided that the sub-contractor's contract is on terms which are substantially the same as those set out in this DPA including the Appendices; and
      2. provided that the sub-contractor's contract terminates automatically on termination of this DPA for any reason.
      3. Supplier accepts full responsibility for compliance with the terms of this DPA and the Agreement by Supplier Affiliates and Sub-processors.
2. **Warranties.** 
   1. Supplier shall guarantee that it will implement and maintain appropriate technical and organizational measures to meet the applicable data protection requirements.
   2. Supplier guarantees that it will only use the Personal Data for the purposes for which the data controller provided the access to or transferred the Personal Data to the Supplier.
   3. Supplier shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Supplier shall ensure that such confidentiality obligations survive the termination of the personnel engagement.
   4. Customer guarantees that the processing of Special categories of personal data if any is being performed under the prior consent of the data subject for such processing pursuant to the requirements of data protection legislation.

1. **Indemnification.** 
   1. The Customer shall indemnify and keep indemnified the Supplier against all claims, proceedings or actions brought by a competent public authority and/or an individual against the Supplier with respect to the Processing by Supplier as a processor and/or sub-processor and shall indemnify and keep indemnified the Supplier against all claims, proceedings or actions brought against the Supplier arising out of any breach of confidentiality, integrity or availability by the Customer of its data protection obligations under the Agreement.
   2. The Customer shall indemnify and keep indemnified the Supplier against all costs related to a data security breach, where that breach was caused by or attributable to Customer’s breach of the Agreement, including Customer’s security obligations under the Agreement.
2. **Confidentiality.** 
   1. Supplier agrees that the details of this DPA are not publicly known and constitute Customer’s Confidential Information under the confidentiality provisions of the Agreement.

1. **Compliance with laws.** 
   1. Each Party will comply with all laws, rules and regulations applicable to it and binding on it, including all Data Protection Laws. Each Party is responsible for complying with their respective obligations of the Controller and Processor as stipulated under the GDPR.

1. **Governing law.** 
   1. This DPA is governed by the laws of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**CUSTOMER SUPPLIER**

[[s|1]]

Please sign above the line Please sign above the line

Date: [[d|0 ]] Date: [[d|1 ]]

Represented by: Represented by: [[t|1|n: Full Name

Title: Title: [

# Appendix 1

# To Supplier Data Processing Agreement as of \_\_ March 2018

# Standard Contractual Clauses

|  |  |
| --- | --- |
| \_\_ March 2018 |  |

[*These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).*]

**Standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council**

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

Name of the data exporting organization: **\_\_\_\_\_\_\_\_\_\_\_**

Address: **\_\_\_\_\_\_\_\_\_\_\_**

Tel.:**\_\_\_\_\_\_\_\_\_\_\_; fax: \_\_\_\_\_\_\_\_\_\_\_ ; e-mail \_\_\_\_\_\_\_\_\_\_\_**

Other information needed to identify the organization **N/A**

**(the data exporter)**

And

Name of the data importing organisation: **Crowdin Inc.**

Address: 8 The Green Dover, DE 19901

Tel.: **\_\_\_\_\_\_\_\_\_\_\_**; e-mail: **\_\_\_\_\_\_\_\_\_\_\_**

Other information needed to identify the organisation:

registration number **364861388**

**(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:

1. *'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;
2. '*the data exporter'* means the controller who transfers the personal data;
3. *'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;
4. *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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;
5. '*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;
6. *'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.

1. The data subject can enforce against the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
2. 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:

1. 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;
2. 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;

1. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
2. 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;
3. that it will ensure compliance with the security measures;
4. 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;
5. to forward any notification received from the data importer or any sub-processor 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;
6. 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;
7. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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
8. that it will ensure compliance with Clause 4(a) to (i).

*Clause 5*

***Obligations of the data importer****[[1]](#footnote-1)*

The data importer agrees and warrants:

1. 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;
2. 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;
3. 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:

* 1. 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,
  2. any accidental or unauthorised access, and
  3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

1. 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;
2. 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;

1. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, 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;
2. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
3. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
4. to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor of its obligations in order to avoid its own liabilities.

1. 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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:
   1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   2. 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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, namely \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

*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*

## *Sub-processing*

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[[2]](#footnote-2). Where the sub-processor 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 sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing 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, namely \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
4. The data exporter shall keep a list of sub-processing 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 sub-processor 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 sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

Name (written out in full): **\_\_\_\_\_\_\_\_\_\_\_**

Position: **\_\_\_\_\_\_\_\_\_\_\_**

Address: **\_\_\_\_\_\_\_\_\_\_\_**

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

Signature……………………………………….

### (stamp of organisation)

**On behalf of the data importer:**

Name (written out in full): **\_\_\_\_\_\_\_\_\_\_\_**

Position: **\_\_\_\_\_\_\_\_\_\_\_** Address: **\_\_\_\_\_\_\_\_\_\_**

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

Signature……………………………………….

(stamp of organisation)

# Appendix 2

# To Supplier Data Processing Agreement as of \_\_ March 2018

# Details of the Transfer

|  |  |
| --- | --- |
| \_\_ March 2018 |  |

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

**Nature of processing**

The processing activity is of the following nature**:**

The data will be uploaded by data exporter to data importer’s platform (Software under the Agreement) where it will be stored and used by the data exporter pursuant to the terms of the Agreement.

**Purpose of processing**

The purpose of processing of the Personal Data is set by the data exporter and implies the performance and operation of the data exporter’s software via the use of the software provided by data importer as set in the Agreement, as well as the performance of the Agreement.

Processing of personal data is strictly limited to what is required for performance of the Agreement. Supplier guarantees that it will only use the personal data for the purposes for which it is provided. Supplier must not process personal data for improving the Services unless such processing is on an anonymized and aggregated basis and does not identify Customer or data subjects.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

Crowdin Inc. (data importer) is a provider of translation and localization software platform for software development and product companies.

**Data subjects**

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Categories of data**

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

Data exporter may submit Personal Data to the data importer`s Software (as defined under the Agreement), the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

[*Please review and correct if the list is not full or accurate.*]

* General information

first and last name;

contact information (email);

address details;

connection data.

* Localisation data.
* Data that is uploaded by Customer to be translated, could include any kind of personal information.
* Usage data:

visits;

browser details;

time stamps;

location;

device.

Personal information contained agreements between the data importer and the data exporter.

**Special categories of data (if appropriate)**

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

Data exporter may not submit special categories of data to the Software (as defined in the Agreement).

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

Data importer shall process the personal data upon the instruction of the data exporter in accordance with the terms of the Agreement via the following ways of processing:  recording, organization, structuring, adaptation or alteration, retrieval, dissemination or otherwise making available, alignment or combination, restriction, erasure.

**Access to the personal data**

Once the personal data has been transferred to the data importer, the following categories of employees and third parties will have access to the personal data (specify the location of the employees and third parties):

The following categories of employees and third parties will have access to the personal data:

Crowdin Inc. employees that may imply the transfer of Personal Data to \_\_\_\_\_\_\_\_\_\_\_\_\_\_;

Crowdin Inc. contractors that are engaged to the provision of services and act as the sub-processors that may imply the transfer of Personal Data to \_\_\_\_\_\_\_\_\_\_\_\_\_\_;

Google Inc., with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043;

Amazon Web Services, Inc. 1200 12th Avenue South, Suite 1200, Seattle, WA 98144 United States;

The relevant agreements with the terms of processing of the personal data shall be executed between the data importer and all the sub-processors as required by this Agreement.

By signing this DPA the data exporter gives its written consent (authorization) for the engagement (subcontracting) of the subcontractors by the data importer for the provision of software development services that imply processing operations of the data importer pursuant to the Agreement. The data importer shall sign the relevant data processing agreements with all the sub-processors that will comply with the requirements of this Agreement.

**Location of personal data**

Data importer will process and store the personal data in the following locations:

8 The Green Dover, DE 19901, Delaware, USA.

**Duration of processing**

The personal data transferred will be processed for the following time frame:

The personal data will be processed throughout the Agreement’s validity term –  for a period of \_\_\_ (\_\_\_\_\_\_\_\_\_) \_\_\_\_\_\_\_\_ (the Effective Date) or until terminated as provided in the Agreement.

**Retention of personal data**

The personal data will be retained by the data importer for the following time frame:

Data importer shall not retain data after the termination of the provision of services pursuant to the Agreement with the data exporter, unless Union or Member State law requires storage.

**List of Sub-processors**

Crowdin Inc. contractors that are engaged to the provision of services and act as the sub-processors (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_).

Google Inc., with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043;

Amazon Web Services, Inc. 1200 12th Avenue South, Suite 1200, Seattle, WA 98144 United States.

**Compliance with laws**

Each Party will comply with all laws, rules and regulations applicable to it and binding on it, including all applicable data protection laws. Each Party is responsible for complying with their respective obligations of the Data Exporter and Data Importer as stipulated under Directive 95/46/EC until it is repealed and the respective obligations of the Controller and Processor under the General Data Protection Regulation when it comes into effect.

**Confidentiality**

Personal data constitutes Confidential Information and the processing of personal data is subject to the confidentiality obligations contained in the Agreement.

DATA EXPORTER

Name: ………………………………

Authorized Signature ……………………

DATA IMPORTER

Name: ……………………….

Authorized Signature …………………

**Appendix 3**

# To Supplier Data Processing Agreement as of \_\_ March 2018

# Security

|  |  |
| --- | --- |
| \_\_ March 2018 |  |

This Appendix forms part of the Clauses and must be completed and signed by the parties **Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

### **Confidentiality:**

Crowdin signs NDA with every employee and contractor;

*Physical Access Control:*

Crowdin ensures that no unauthorized access to the facilities where data will be processed is possible. Crowdin uses facility security services and/or entrance control staff, alarm systems and video control systems.

*Electronic Access Control*

Crowdin takes measures in order that no unauthorized use of the data processing and data storage systems is possible: the use of secure passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media is a must.

*Operational Security*

Internal processes in our data centers comply with the Multi-Tier Cloud Security Standard (MTCS SS 584) Level-3 (CSP) certification requirements.

Crowdin’s software is regularly audited by security specialists. Systems access is admitted and tracked for auditing purposes. Crowdin ensures fully documented change-management procedures. Crowdin code is written by Crowdin’s developers based on OWASP best practices and recommendations.

*Internal access control (permissions for user rights of access to and amendment of data)*

Crowdin takes measures in order that that no unauthorized reading, copying, changes or deletions of data within the system, e.g. rights authorisation concept, need-based rights of access;

*Personnel training*

Crowdin arranges and provides training for its personnel and contractors regarding confidentiality, integrity and availability and resilience of processing systems and services within the GDPR compliance;

*Isolation control*

Crowdin ensures the isolated processing of data, which is collected for differing purposes

### **Integrity measures**

*Data transfer control*

Crowdin takes measures in order that no unauthorized reading, copying, changes or deletions of data with electronic transfer or transport, transfer within the secured internet channels

*Data entry control*

Crowdin ensures verification, whether and by whom personal data is entered into a data processing system, is changed or deleted, e.g.: Logging control

### **Availability and Resilience measures**

*Availability control*

#### File System and Backups

At the system layer, the servers are deployed with redundant network cards, redundant power supplies, and redundant disk storage. Secure data centers have generator backup systems and UPS for power and various entry points for key utilities and communication facilities. Regular backups are made and stored off-site in different Amazon AWS datacenter.

### **Procedures for regular testing, assessment and evaluation**

Crowdin provides regular checks in order to identify of the personal data flows on the platform the data importer provides in respect of what and how information is stored, accessed, used and processed in any other manner.

Crowdin conducts periodical compliance checks with the requirements of this DPA as well as the requirements of the current data protection legislation.

Crowdin provides regular identification and record of the data processing risks in relation to the data importer’s contractual and legislative obligations;

Crowdin takes measures to mitigate the risk after its identification.

*Contract Control*

Crowdin takes measures in order that no third-party processes data as per Article 28 GDPR without corresponding instructions from the data controller, e.g.: clear and unambiguous contractual arrangements, duty of pre-evaluation, supervisory follow-up checks.

***Liability***

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:

the data exporter promptly notifying the data importer of a claim; and

the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

DATA EXPORTER

Name: ………………………………

Authorized Signature ……………………

DATA IMPORTER

Name: ……………………….

Authorized Signature …………………

1. Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter* *alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements. [↑](#footnote-ref-1)
2. This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. [↑](#footnote-ref-2)