Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Name

CVR-number

Address

Postcode and city

Country

(the data controller)

and

EasyTranslate A/S
CVR no.: 33240562
Bygmestervej 10, 2TH
2400 Copenhagen
Denmark

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Data Processing Agreement (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

easytranslate

Table of Contents

1. Preamble

1. This Data Processing Agreement (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).If the data controller has no establishment in the European Union or the EEA for the purposes of the processing activity and the processing activity does not fall under the territorial scope of the GDPR as per Article 3(2), the data processor's obligations in this data processing agreement shall be interpreted and limited to take into account that the data controller is not subject to obligations under GDPR.

3. In the context of the provision of language services the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Five appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. If the data controller is established in a non-EEA country which has not been deemed by the EU Commission to provide adequate protection of personal data through an adequacy decision, the parties by virtue of accepting this Data Processing Agreement agree to be bound by the Standard Contractual Clauses (SCC's) for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council – module 4 (P2C) (COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021) as attached as Appendix E.

11. The Clauses along with appendices, shall be retained in writing, including electronically, by both parties.

12. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions. In such cases the Parties shall find a solution.

3. In case the data controller maintains its instructions, the parties must with a positive, cooperative and responsible attitude initiate negotiation to resolve the dispute.

4. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5. Security of processing

1. Article 32 GDPR stipulates that, 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, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform the data controller in writing of any intended changes concerning the addition or replacement of sub-processors thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The data processor will notify the data controller via the data processor's platform.

3. If the data controller does not approve of a new sub-processor, then the data controller may terminate its agreement with the data processor by providing, before the end of the relevant notice period, written notice of termination. The data controller may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit the data processor to re-evaluate any such new sub-processor based on the applicable concerns.

4. The list of sub-processors already authorised by the data controller can be found in Appendix B.

5. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, similar data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

6. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organisation.

   b. transfer the processing of personal data to a sub-processor in a third country.

   c. have the personal data processed in by the data processor in a third country.

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 8.1. and 8.2.

9. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 8(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

2. The data processor commits to exclusively process the personal data for the purposes and duration provided for by such law and under the strict applicable conditions.

11. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory

authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12. The parties' agreement on other terms

1. The parties may agree to other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13. Commencement and termination

1. The Clauses shall become effective once the data processor receives validly completed and counter-signed Clauses at gdpr@easytranslate.com by the data controller. The data processor will provide the data controller with an email confirming receipt of the counter-signed Clauses indicating the Clauses' effective date.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the Terms & Conditions are terminated and the personal data is deleted or returned to the data controller pursuant to Clause 10.1. and Appendix C.4., the Clauses will be considered terminated automatically.

5. Signature

On behalf of the data controller

Name
Position
Date
Signature

On behalf of the data processor

Name	Sabrina Eisele Jensen
Position	Compliance Manager
Date	21.09.2022
Signature	

14. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name
Position
Telephone
E-mail

Name	Sabrina Eisele Jensen
Position	Compliance Manager
E-mail	sabrinae@easytranslate.com

● Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

If the data controller applies the data processor's Translation Service Platform services:
To perform translation services of source files on behalf of the data controller. Source files can contain all kinds of personal data which is reflected in the section below.

To perform other language services on behalf of the data controller, such as DTP, editing, interpreting, proofreading, subtitling, transcribing, voice-over, or other, where source files can contain all kinds of personal data which is reflected in the section below. These language services are covered by the translation service reference in the document.

If the data controller applies the data processor's Localisation Software Platform services:
To offer the data controller to use tools and services offered by the data processor in its Software platform, including:

- Machine translation tools allowing the data controller to upload source files and have the files machine translated to any chosen language
- Content generation tool creating full texts based on data controller's key words
- To liaise with external translators with whom the data controller can enter into direct contractual relationships, and to build an own team of freelance translators, share content, information, videos and guidelines etc.
- Content edit tool
- Hosting of uploaded source files and translations and edits thereof
- Ability to use the tools 'Roles and Permissions', 'Wallet and Payments' and other tools which at any time is made available to data controller in the platform

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Collection, storage, translation, return, deletion and anonymization.

A.3. The processing includes the following types of personal data about data subjects:

The personal data processed will depend on what source files the data controller instructs the data processor to translate. **The data controller is encouraged to anonymize or pseudonymize source files and other content as much as possible prior to disclosing to the data processor and uploading to the platform**.

Types of personal data processed in connection with the provision of translation services may include any personal data included in source files and other content which the data controller in its own discretion chooses to disclose to the data processor or upload to the platform. As such the personal data may include ordinary as well as special categories of data of any nature.

A.4. Processing includes the following categories of data subject:

The data subjects whose personal data is processed will depend on what source files the data controller instructs the data processor to translate. The data controller may include any data subject whose personal data may be included in source files and other content which the data controller in its own discretion chooses to disclose to the data processor or upload to the platform.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

During the term of the agreement, c.f. the Terms & Conditions, between the data controller and data processor. In the platform account settings, the data controller has full control over any data and can at any time access, edit, export, and delete data, at the click of a button.

● Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the listed sub-processors on the data processor's website that may be accessed here.

The data controller shall on the commencement of the Clauses authorise the use of these sub-processors for the processing described for that party.

Whenever the data controller places an order for translation or other language services with the data processor, the data controller acknowledges that the instruction for translation or other language services to a specific language, also constitutes 1) the data controllers approval of the processors engagement of a sub processor qualified to perform the translation or other language service in the specific language, and 2) an instruction to transfer any personal data included in the source file submitted by the data controller to the specific country in which the engaged sub processor is performing the services, including where the services are performed in a non-EEA country. The data processor will inform the data controller of the identity and the location of the sub processor.

The data controller is recommended to anonymize/or pseudonymize any source file prior to transferring it to the data processor so that it does not include identifiable personal data.

● Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

If the data controller applies the data processors Translation Service Platform services:

- To receive, host, access and translate source files and other content and return the same to the data controller.
- To make source files and other content available to Sub-processors, (including external translators) for translation, including in jurisdictions outside the EEA.
- To delete data.

If the data controller applies the data processors Localisation Software Platform services:

- To facilitate the data controller's upload and hosting of source files and other content and translations thereof in the data processors platform.
- To allow the data controller to use various automatic services including Machine translation, Content generation and edit tools (AI and machine learning software).
- To facilitate the data controllers in platform communication and at the discretion of the data controller sharing of content, information, videos and guidelines etc. with freelance translators at the data controllers choosing.
- To process the data controller's data and source files in tools made available to the data controller in the platform.
- To delete data.

C.2. Security of processing

The level of security shall take into account that the processing may involve confidential and special categories of personal data. The data controller is however recommended to anonymize/or pseudonymize any source file prior to transferring it to the data processor so that it does not include identifiable personal data.

Information Security. The data processor will maintain information security (including the adoption and enforcement of internal policies and procedures) designed to (a) help the data controller to secure personal data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the data, and (c) minimise security risks, including through risk assessment and regular testing. The data processor will designate one or more employees to coordinate and be accountable for the information security. The information security will include the following measures:

Network Security. The data processor's networks are segmented and will be electronically accessible to employees, contractors and any other person as necessary. The data processor will maintain access controls and policies to manage what access is allowed to the network, including the use of firewalls or functionally equivalent technology.

Ability to restore the availability and access to personal data in a timely manner in the event of a technical incident. The data processor assures redundant software architecture for high service up-time. All data is backed up through daily full backups to a highly durable storage.

Monitoring and testing. The data processor is monitoring and testing the technical configuration on a continuous basis through the continuous performance of vulnerability scans, the regular performance of penetration tests, and similar.

Protection of data during transmission and storage. The data processor assures encryption of the data in transit and storage on its platform based on recognized encryption standards.

Logging. The data processor logs user activities in its systems, databases and networks used to process and transmit the personal data. The logs are monitored.

Access. The data processor has implemented Role-Based Access Control (RBAC) on a need-to-know basis to its systems and databases. Access to systems and databases in which the personal data are being processed can only be obtained through two- or multifactor authentication.

Physical Security. All server locations are physically secured. The data processor further assures Physical Access Control to prevent unauthorised entrance to server locations. Passage requires either electronic access control validation (e.g. card access systems, etc.) or validation by human personnel (e.g. contract or in-house security guard service, receptionist, etc.). The data processor maintains electronic intrusion detection systems designed to detect unauthorised access.

Home/remote working. The data processor assures that employees working from home or remotely keep the same confidentiality standards processing personal data as given in the main processing location (the main office). All devices used to work from home or remotely fulfil the same security requirements as devices used in the main processing location.

Sub-data processors. The sub-data processors will maintain information security designed to (a) help EasyTranslate to secure personal data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the data, and (c) minimise security risks. EasyTranslate therefore requires the sub-processors to maintain technical and organizational measures, thereunder secure networks usage, protection of data during processing, access management, and confidentiality.

Continued Evaluation. The data processor will conduct periodic reviews of its technical and organisational measures against industry security standards and its policies and procedures. The data processor will continually evaluate its information security to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 8.1. and 8.2. by implementing the following technical and organisational measures:

In general, the data controller may accommodate data subject requests in the data processor's platform directly without the assistance from the data processor. Should the assistance from the data processor be required then the data controller must compensate the data processor for any time spent on this in accordance with the data processor's current hourly rate for IT support.

C.4. Storage period/erasure procedures

Source and translation files are stored for a maximum period of one year from when they were first uploaded unless the data controller in its own discretion chooses to delete files before. The data controller can opt-out from the automatic file erasure in the platform account settings.

Upon termination of the provision of personal data processing services, the data processor will erase the personal data in accordance with Clause 10.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such

modification shall be documented and kept in writing, including electronically, in connection with the Clauses. The data are erased no later than one year from the date of termination.

The data controller has the opportunity to export the personal data before the end of the contract.

C.5. Processing location

The sub-data processor's individual processing locations are listed on the data processor's website, cf. Appendix B.1.

C.6. Instruction on the transfer of personal data to third countries

The processor is instructed to transfer personal data via its sub-data processors to the listed third countries on the data processor's website, cf. Appendix B.1.

Whenever the data controller places an order for translation or other language services with the data processor, the data controller acknowledges that the instruction for translation or other language services to a specific language, also constitutes 1) the data controllers approval of the processors engagement of a sub processor qualified to perform the translation or other language service in the specific language, and 2) an instruction to transfer any personal data included in the source file submitted by the data controller to the specific country in which the engaged sub processor is performing the services, including where the services are performed in a non-EEA country. The data processor will inform the data controller of the identity and the location of the sub processor.

The data controller is recommended to anonymize/or pseudonymize any source file prior to transferring it to the data processor so that it does not include identifiable personal data.

The appropriate safeguards to transfer personal data to third countries are secured by the processor having concluded EU Commissions Standard Contract Clauses (module 3 – P2P) (cf. article 46 of the GDPR) with all of its sub-data processors.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data controller will carry out an appropriate audit of the data processor to ensure that the data processor complies with the data processor's obligations under this Data Processing Agreement and the Data Protection Regulation.

The data controller or the data controller's representative shall have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

The data controller's costs, if applicable, relating to its control of the data processor shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection. The data controller must, however, compensate the data processor for any time spent on this in accordance with the data processor's current hourly rate for IT support.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

On the basis of the specific outsourced processing activities, the data processor will carry out an appropriate audit of the sub-data processors to ensure that the sub-data processor complies with the data processor's obligations under this Data Processing Agreement and the Data Protection Regulation.

The data controller may at any time request documentation for the audit carried out.

- **Appendix D The parties' terms of agreement on other subjects**

The data processor shall be compensated by the data controller on a time and material basis for all the time the data processor assists the data controller with the obligations described in Clauses 8 and 9 and appendix C.7 in accordance with the data processor's current hourly rate for IT support. Furthermore, should the data controller make any changes to its instruction such changes will only be accepted provided they are technically feasible and subject to separate payment to the data processor.

- **Appendix E Standard Contractual Clauses**

STANDARD CONTRACTUAL CLAUSES (MODULE 4 - PROCESSOR TO CONTROLLER)

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) and Clause 8.3(b);

(iii) [*Intentionally left blank*];

(iv) [*Intentionally left blank*];

(v) Clause 13;

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

(vii) Clause 16(e); and

(viii) Clause 18.

(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 exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data

exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

[*Intentionally left blank*].

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

Clause 13

Supervision

[*Intentionally left blank*].

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

Clause 14

Local laws and practices affecting compliance with the Clauses

[*Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU*]

Clause 15

Obligations of the data importer in case of access by public authorities

[*Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU*]

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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Denmark.

ANNEX I

A. LIST OF PARTIES

Data exporter:

Name: EasyTranslate A/S

Address: Bygmestervej 10, 2. th, 2400 København NV

Contact person's name, position and contact details:

Sabrina Eisele Jensen, Compliance Manager, sabrinae@easytranslate.com.

Data Protection officer's (if any) name, position, and contact details: n/a

EU representative's (if any) name, position, and contact details: n/a

Activities relevant to the data transferred under these Clauses: Provision of translation services of source files provided the by data importer and returning translated files to the data importer.

Signature and date: 21.09.2022

Data exporter / Processor

Data importer:

Name and Address: EasyTranslate's (data exporter's) customer as identified by the customer itself in its order request for translation or other services as submitted in the data exporter's Translation Service Platform or Localisation Software Platform.

Activities relevant to the data transferred under these Clauses: Access to the data exporters platform, usage of the services of the platform and return of the translated/edited source files.

Signature and date:

Data importer / Controller

B. DESCRIPTION OF TRANSFER

The data exporter will transfer (return) to the data importer translated or otherwise edited etc, versions of source files originally provided by the data importer to the data exporter. The data exporter will not combine the personal data received from the data importer with personal data collected by the processor in the EU.

Categories of data subjects whose personal data is transferred

The data subjects whose personal data is processed will depend on what source files the data controller (data importer) instructs EasyTranslate (data exporter) to translate or include in other language services. The data subject may include any data subject whose personal data may be included in source files and other content which the data controller (data importer) in its own discretion chooses to disclose to the data processor or upload to the platform.

Categories of personal data transferred

The personal data processed will depend on what source files the data controller (data importer) instructs EasyTranslate (data exporter) to translate or include in other language services. Types of personal data processed in connection with the provision of translation services may include any personal data included in source files and other content which the data controller (data importer) in its own discretion chooses to disclose to EasyTranslate (data exporter) or upload to the platform. As such the personal data may include ordinary as well as special categories of data of any nature.

The data controller (data importer) is encouraged to anonymize or pseudonymize source files and other content as much as possible prior to disclosing to EasyTranslate (data exporter).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

We refer to point above, *"Categories of personal data transferred".*

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous access to the data importers own source files and translated files in the Translation Service Platform and Localisation Software Platform and one-off transfer (return) of the translated or edited versions of the data importers source files.

Nature of the processing

Collection, storage, translation, return, and deletion and anonymization.

Purpose(s) of the data transfer and further processing

The data exporter will transfer (return) to the data importer translated or otherwise edited etc, versions of source files originally provided by the data importer to the data exporter.

The data exporters Services:

- To perform translation services of source files on behalf of the data importer and provide continuous access to the Translation Service Platform and Localisation Software Platform.
- To perform other language services to the data importer such as DTP, editing, interpreting, proofreading, subtitling, transcribing, voice over, or other.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

Source and translation files are stored by the data exporter for a maximum period of one year from when they were first uploaded unless the data controller (data importer) in its own discretion chooses to delete files before. Source and translation files are deleted upon termination of the data importers user account.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

n/a.