Standard Contractual Clauses

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

between

Company name

Company CVR

Company address

Company postal code & city

Company country

(the data controller)

and

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

(the data processor)

each a ‘party’; together ‘the parties’

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

1. **Table of Contents**

2. Preamble 3
3. The rights and obligations of the data controller 3
4. The data processor acts according to instructions 4
5. Confidentiality 4
6. Security of processing 4
7. Use of sub-processors 5
8. Transfer of data to third countries or international organisations 6
9. Assistance to the data controller 7
10. Notification of personal data breach 8
11. Erasure and return of data 8
12. Audit and inspection 8
13. The parties' agreement on other terms 9
14. Commencement and termination 9
15. Data controller and data processor contacts/contact points 10

- Appendix A Information about the processing 11
- Appendix B Authorised sub-processors 12
- Appendix C Instruction pertaining to the use of personal data 13
- Appendix D The parties' terms of agreement on other subjects 16

2. Preamble

1. These Contractual Clauses (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).

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

11. 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.

3. 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.

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

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.

4. 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 case 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.

5. 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.

6. 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.

   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 require 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.

7. 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 in writing the data controller 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). Data processor will notify the data controller via the account setting of the data controller on 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.

8. 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 organization

   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.

9. 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 9.1. and 9.2.

10. 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 9(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.

11. 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 this law and under the strict applicable conditions.

12. 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.

13. The parties' agreement on other terms

1. The parties may agree 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.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

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 11.1. and Appendix C.4., the Clauses will be considered terminated automatically.

5. Signature

On behalf of the data controller

Name

Job title

Date

Signature

On behalf of the data processor

Name

Job title

Date

Signature

15. 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
Job title
Telephone
E-mail

Name
Job title
Telephone
E-mail

● 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:

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.

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 and 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.

Types of personal data processed in connection with provision of translation services may include

- General personal information, including name, date of birth, place of birth, address, telephone number, and e-mail address
- Confidential information such as personal identification number
- Information on criminal record and violations of the law
- Special categories of personal data, including race-related or ethnic background, political, religious or philosophical beliefs, trade union membership, details related to health or sexual orientation, and genetic data

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 subject may include the following categories:

- Employees of the data controller
- Suppliers of the data controller
- Customers of the data controller
- Children, 0-18 years of age.

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.

● 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.

● 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:

The data processor shall translate the personal 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.

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 Intrusion Prevention System and Intrusion Detection System (IPS & IDS), 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 Bases 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 than 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.

Continued Evaluation. The data processor will conduct periodic reviews of its technical and organizational 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 9.1. and 9.2. 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

Below the overview of the storage period/erasure procedures for each product:

EasyOrder
The EasyOrder storage periods and erasure procedures depend on the behaviour of the data controller.

- If the data controller empties the basket before completing the order in the EasyOrder flow, the files are immediately deleted from the EasyOrder flow and erased after 30 days from when they were first uploaded.
- If the data controller leaves with an open basket before completing the order in the EasyOrder flow, the files are accessible for 30 days in the EasyOrder flow to complete the order, and are erased after 60 days from then they were first uploaded.
- If the data controller completes the order in the EasyOrder flow, the translation file is accessible to download for 30 days in the EasyOrder dashboard from when the translation was delivered. The source and translation files are erased after a maximum period of one year from when they were first uploaded.

Source and translation files are stored for a maximum period of one year from when they were first uploaded. The data controller can opt out from the automatic file erasure in the platform account settings. The source and translation files are then stored, together with the Translation Memory, Term Base, and the personal data associated with the platform user account until the termination of the provision of personal data processing services.

Upon termination of the provision of personal data processing services, the data processor will erase the personal data in accordance with Clause 11.1., 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.

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. Clause 7. The legal basis for the transfer is the Commission's standard contractual clauses.

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 T / M basis for all the time the data processor assists the data controller with the obligations described in Clauses 8 and 9 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.