DATA PROCESSING AGREEMENT

between

Company name

CVR number

Company address

Postal code & town/city

Country
(the “Data Controller”)

and

EasyTranslate

CVR no.: 33240562

Sundkaj 153, 1.

2150 Nordhavn

The “Data Processor”

(The Data Controller and Data Processor are hereinafter jointly called “the Parties” and individually a “Party”)

Appendices to the Data Processing Agreement

Appendix 1	The Principle Service
Appendix 2	Technical and organisational security criteria and guarantees
Appendix 3	Proof of observance
Appendix 4	Specific assistance
Appendix 5	The Data Controller's undertakings
Appendix 6	Sub-Data Processors
Appendix 7	Transfer to Third Countries and international organisations

1 Background and Purpose

1.1 The Parties have entered agreed provision of certain services from the Data Processor to the Data Controller as set out in the separate contract between the Parties and Appendix 1 to this agreement ("the Principle Services").

1.2 In this connection, the Data Processor will process personal data on behalf of the Data Controller, and the Parties have consequently entered into this agreement with its appendices ("the Data Processing Agreement").

1.3 The Data Processing Agreement has been drawn up with regard to observance by the Parties of Article 28 (3) of 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), which sets out specific requirements as to the content of a Data Processing Agreement.

2 Scope

2.1 The Data Processor is authorised to undertake the processing of the personal data specified in Appendix 1 on behalf of the Data Controller, on the terms set out in the Data Processing Agreement.

2.2 The Data Processor can only process personal data according to the documented instructions provided by the Data Controller ("the Instructions") unless required in accordance with EU law or the national law of member states to which the Data Processor is subject. In such instances, the Data Processor shall inform the Data Controller of the correct legal requirements before commencing processing, unless that law prevents such notification with regard to important social interests.

2.3 This Data Processing Agreement and its appendices comprise the Instructions at the time the Agreement was signed. The Instructions state that the Data Processor may undertake all processing necessary to be able to provide the Principle Service, until otherwise stipulated by the Data Controller.

3 Duration

3.1 The Data Processing Agreement shall remain effective until either (a) the agreement on provision of the Principle Services expires, or (b) the Data Processing Agreement is terminated or cancelled.

4 The Data Processor's undertakings

4.1 Technical and organisational security precautions

4.1.1 In conjunction with the Data Processor processing personal data for the Data Controller, the Data Processor is responsible for provision of the necessary (a) technical and (b) organisational security precautions.

4.1.2 Such precautions shall be implemented with regard to the actual technical level, cost of implementation and their nature, scope, composition and purpose, along with the risks of varying probability and severity to the rights of legal persons and their rights of freedom, and the types of personal data specified in Appendix 1.

4.1.3 The Parties agree that the technical and organisational security precautions set out in (a) Appendix 2 to the Data Processing Agreement, and (b) the agreement(s) on provision of the Principle Services are sufficient with regard to ensuring a suitable level of security at the time of the signing of the Data Processing Agreement. The Data Processor shall nevertheless be responsible for regularly ensuring that the implemented (a) technical and (b) organisational precautions are sufficient to ensure a suitable level of security.

4.2 Employees

4.2.1 The Data Processor shall ensure that the employees processing personal data on its behalf have undertaken to maintain confidentiality or are subject to a suitable mandatory duty of confidentiality laid down by law.

4.2.2 The Data Processor shall ensure that access to the personal data shall be limited to those employees for whom it is necessary to process personal data to be able to fulfil the Data Processor's contractual undertakings to the Data Controller.

4.2.3 The Data Processor shall ensure that any employees processing personal data on its behalf only process them in accordance with the Instructions.

4.3 Proof of observance

4.3.1 The Data Processor shall make available all details necessary to prove observance of the requirements in the Data Processing Agreement to the Data Controller, and permit and contribute to audits, including inspections, performed by the Data Controller or an auditor authorised by the Data Controller. Such a request shall be responded to without undue delay.

4.3.2 With regard to clause 4.3.1 the Data Processor shall immediately inform the Data Controller if it deems an instruction to be in violation of data protection law, or the data protection provisions in other EU laws or national laws.

4.3.3 Specific and additional requirements for proof of observance are set out in Appendix 3.

4.4 **Breach of security**

4.4.1. The Data Processor shall notify the Data Controller without undue delay if becoming aware of a breach occurring in personal data security.

4.4.2. Such notification shall contain the actual circumstances of the breach of personal data security, its effect and the measures put into place or planned to remedy the situation.

4.5 **Assistance**

4.5.1 With regard to the nature of the processing, the Data Processor shall assist the Data Controller to the extent possible with the aid of suitable technical and organisational precautions to fulfil the Data Controller's undertaking to respond to requests from data subjects to exercise their rights. This entails that the Data Processor shall assist the Data Controller to the extent possible to ensure that the Data Controller shall ensure observance of

a. the duty to inform when collecting personal data from the data subjects
b. the duty to inform if personal data have not been collected from the data subject
c. the data subject's right of access
d. the right to rectify
e. the right to erasure/to be forgotten
f. the right to restrict processing
g. the duty to inform in connection with the rectification or erasure of personal data, or limitation of processing
h. the right data portability
i. the right to object
j. the right to object to the result of automated individual decision making, including profiling

4.5.2 With regard to the nature of the processing and the data accessible to the Data Processor, the Data Processor shall furthermore assist the Data Controller to ensure observance of undertakings concerning the Data Controller's:

a) Processing security,

b) Reporting breaches of personal data security to the supervisory authorities,

c) Reporting breaches of personal data security to the data subject,

d) Consequence analyses concerning data protection, and

e) Prior consultations.

5 The Data Controller's undertakings

5.1 The Data Controller has the undertakings set out in Appendix 5 and the agreement(s) on provision of the Principle Services.

6 Sub-Data Processors

6.1 The Data Processor can only use a third party for processing personal data for the Data Controller ("Sub-Data Processors") to the extent set out in the (always up-to-date) list of Sub-Data Processors

https://www.easytranslate.com/en/dpa-vendors/

6.2 The Data Processor and Sub-Data Processor shall enter into a written agreement placing the Sub-Data Processor under the same data protection undertakings as apply to the Data Processor (including in pursuance of this Data Processing Agreement).

6.3 The Sub-Data Processor shall furthermore only act on the Instructions from the Data Controller. All communication with the Sub-Data Processor shall be handled by the Data Processor, unless otherwise separately agreed.

6.4 If a Sub-Data Processor fails to fulfil the Instructions, the Data Controller can prohibit the use of that Sub-Data Processor.

6.5 The Data Processor is directly responsible for processing of personal data by the Sub-Data Processor in the same manner as if such processing was performed by the Data Processor itself.

7 Transfer to Third Countries and international organisations

7.1 The Data Processor can only transfer personal data to a country outside the European Union or EEA (a "Third Country") or international organisations when stipulated in (a) Appendix 7 to the Data Processing Agreement, or (b) the Instructions from the Data Controller.

7.2 Transfer of personal data can only be effected in any event if the Data Processor has the necessary grounds to do so, e.g. the EU Commission's Standard Contract Provisions or other legal grounds for transfer.

7.3 If the above grounds permitting transfer require that the Data Controller is a direct party to the same, the Data Processor is authorised to execute transfer on behalf of the Data Controller, e.g. by entering into an agreement to use the EU Commission's Standard Contract Provisions or other legal grounds for transfer on behalf of the Data Controller. The Data Processor shall inform the Data Controller at the earliest opportunity if such authority is used and shall forward a copy of the signed standard contract and indicate corresponding legal grounds for transfer.

7.4 Any regulation applicable in pursuance of the grounds for transfer used shall take priority over the regulation in this Data Processing Agreement, although only in relation to the processing which necessitates the grounds to transfer. Any other processing is solely regulated by this Data Processing Agreement.

8 Payment and Costs

8.1 The Data Processor is entitled to reasonable payment by the hour, and for its other costs incurred for the services performed according to the Data Processing Agreement at the request of the Data Controller. Notwithstanding the above, the Data Processor shall supply the services stated in clause 4.5.1 at no cost to an extent equivalent to 5% of the average annual payment for the Principle Services.

8.2 The Data Processor is entitled to reasonable payment by the hour and other costs incurred for those services performed according to the Data Processing Agreement as a result of changes in the circumstances of the Data Controller, unless caused by changes in data protection law in general, (as opposed to industry- or sector-specific law). Changes in the practices of the authorities shall not be regarded as changes in the law.

8.3 Payment shall be according to agreed hourly rates in the agreement(s) on provision of the Principle Services, and when hourly rates are not agreed therein, shall be according to the Supplier's applicable hourly rates.

8.4 Notwithstanding the above, the Data Processor is entitled to payment for assistance with or implementation of changes to the extent such assistance or change are a direct consequence of the Data Processor's own breach of the Data Processing Agreement.

9 CHANGES to the Instructions

9.1 Prior to changes to the Instructions, the Parties shall discuss to the extent possible, and if possible agree, to such changes, including an implementation date and costs.

9.2 Unless otherwise agreed, the following apply:

a) The Data Processor shall implement changes to the Instructions without undue delay and ensure that such changes are implemented without undue delay in relation to their nature and scope.

b) An estimate of how long implementation will take, and its cost shall be reported to the Data Controller without undue delay.

c) The Data Processors cannot be held liable for non-delivery of the Principle Services when such delivery will be in violation with changed Instructions (including in relation to timing) or delivery in accordance with the changed Instruction is impossible. This can be the case, for example, (i) when the changes cannot be implemented for technical, practical or legal reasons, (ii) the Data Controller explicitly states that the changes shall apply before implementation is possible, or (iii) during the period until the Parties make any necessary changes to the agreement(s) according to the change procedures herein.

10 Other provisions

10.1 General information

10.1.1 Regulation of items dealt with under clause 10 of the agreement(s) on provision of the Principle Services shall also apply to this Data Processing Agreement as if it was an integrated part of such an agreement or agreements. The provisions of clause 10 shall only apply to this Data Processing Agreement when the agreement(s) on provision of the Principle Services directly apply to it.

10.2 Liability and limitation of liability

10.2.1 The Parties are liable in accordance with the general rules of applicable law, although with the limitation applied by clause 10.2. Such limitations only apply if the actions or neglect of a Party can be characterised as deliberate or grossly negligent.

10.2.2 Each Party will not accept any liability for indirect loss and consequential loss, including operational loss, loss of turnover, loss of benefits etc.

10.2.3 Each Party's liability for all cumulative, direct claims in accordance with this Data Processing Agreement, including related to all forms of claims from third parties (including the data subjects), is limited to the total amount of payments due in accordance with the Principle Services for the 24-month period immediately preceding the act that the claim concerns. If the Data Processing Agreement has not been in effect for 24 months, the amount will be equal to that agreed payment for the Principle Services during the period the Data Processing Agreement was in effect divided by the number of months it was in effect and then multiplied by 24.

10.3 Force Majeure

10.3.1 The Data Processor cannot be held liable for circumstances that are normally described as force majeure, including, but not limited to, war, riots, terror, rebellion, strikes, fire, natural disasters, currency restrictions, import or export restrictions, disruption to ordinary traffic, virus,

10.3.2 Force majeure can only apply for the number of days the situation lasts.

10.4 Confidentiality

10.4.1 Information concerning the content of this Data Processing Agreement, the underlying Principle Services, the other Party's business, which has been classified as confidential information when disclosed to the receiving Party, or that by its nature or in general can clearly be regarded as confidential, shall be treated as confidential and with the same care and discretion as the Party's own confidential information. Data, including personal data, always comprises confidential information.

10.4.2 The duty of confidentiality does not apply to information which is, or will be, in the public domain, unless due to a breach of a Party's duty of confidentiality, or information that was already in the receiving Party's possession and not covered by any corresponding duty of confidentiality, or information independently generated by the receiving Party.

11 Termination

11.1 Termination and cancellation

11.1.1 The Data Processing Agreement can only be terminated or cancelled according to the provisions on termination and cancellation in the agreement(s) on provision of the Principle Services.

11.1.2 Termination or cancellation of the Data Processing Agreement can only be accomplished by – and entitling to – concurrent termination or cancellation of parts of the agreement(s) on provision of the Principle Services concerning processing personal data in pursuance of the Data Processing Agreement.

11.1.3 When the agreement(s) on provision of the Principle Services expires, the Data Processing Agreement will remain in effect until those personal data are erased or returned as specified in clause 11.5.

11.2 Effect of termination

11.3 The Data Processor's authority to process personal data on behalf of the Data Controller shall lapse upon expiry of the Data Processing Agreement, regardless of cause.

11.4 The Data Processor shall continue to process the personal data for up to three months after expiry of the Data Processing Agreement to the extent necessary to undertake the necessary mandatory precautions. During the same period, the Data Processor is entitled to back up the personal data in its usual backup procedure. The Data Processor's processing during that period shall be regarded as still being subject to the Instruction.

11.5 The Data Processor and its Sub-Data Processors shall return all personal data they have processed under this Data Processing Agreement to the Data Controller upon expiry of the Data Processing Agreement to the extent the Data Controller is not already in possession of such personal data. The Data Processor shall then erase all personal data from the Data Controller. The Data Controller can request the necessary proof that this has been done.

11.6 Notwithstanding the expiry of the Data Processing Agreement, clauses 10.2, 10.4, 11.4 and 12 shall continue to apply.

12 Disputes

12.1 The Data Processing Agreement is subject to Danish law with the exception of (a) rules that lead to the use of any other law than Danish law, and (b) the UN Convention on Contracts for the International Sale of Goods (CISG).

12.2 If the Parties cannot reach a solution via negotiation, they are entitled to demand that the dispute is resolved by court proceedings in the common courts. The Data Controller's District Court is nominated as the Court of Venue. The rules concerning referral to the High Court and to the Maritime and Commerce Court in the Administration of Justice Act shall apply.

13 precedence

13.1 In the event of contradiction between the Data Processing Agreement and the agreement(s) on provision of the Principle Services, the Data Processing Agreement shall take precedence, unless otherwise directly stated in the Data Processing Agreement.

14 signatures

[●], dated [●]

For the Data Controller

Company name

Name: Name

Title: Title

Signature

For the Data Processor

EasyTranslate A/S

Frederik R. Pedersen

Name: Frederik R. Pedersen
Title: CEO

Stamp

APPENDIX 1

THE PRINCIPLE SERVICE

1 Purpose and Principle Service

1.1 The purpose of processing in pursuance of the Data Processing Agreement is to provide the Principle Service consisting of the following: translation 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.

2 Personal data

2.1 Types of personal data processed in connection with provision of the Principle Service:

a) General personal information, including name, date of birth, place of birth, address, telephone number, and e-mail address;

b) Sensitive 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;

c) Details on criminal record and violations of the law;

d) CPR numbers.

2.2 The category of registered identified or identifiable physical persons covered by the Data Processing Agreement:

e) Employees;

f) Suppliers;

g) Clients;

h) Children, 0-18 years of age.

APPENDIX 2

TECHNICAL AND ORGANISATIONAL SECURITY REQUIREMENTS AND GUARANTEES

1 Specific technical and organisational security criteria and guarantees the Parties:

1.1 The following specific requirements apply to the Data Processor's physical security:

i) The primary location for the supplier is physically secured against unauthorised access;

j) If colleagues work remotely, the physical room is secured such that it is confidential;

k) Infrastructure systems are used which are secure with respect to guaranteed integrity;

l) Use of mobile storage media is forbidden and secured with blocking processes;

m) Printers are secured with role-based codes.

1.2 The following specific requirements apply to the Data Processor's technical security:

n) All traffic between the end user and EasyTranslate's platform is encrypted (HTTPS/SSL);

o) All source files delivered by the client and translations delivered by EasyTranslate are stored on servers in encrypted form (AES-256);

p) All users, i.e. clients, suppliers, and employees are subject to role-based rights management on EasyTranslate's platform to ensure that only relevant persons have access to sensitive personal data;

q) All user passwords are stored in encrypted form (Bcrypt/Blowfish) which cannot be reproduced/read;

r) All employees use two-factor authentication to be able to access the platform;

s) All page views and actions performed on the platform by users, including log-ins and file downloads, are logged in a transaction log. This includes username, time and other relevant metadata relating to the action.

1.3 The following specific requirements apply to the Data Processor's organisational security:

t) All employees and consultants are subject to an NDA;

u) All employees and consultants undergo awareness training with an exam;

v) All employees are instructed in compliant processing via training, guidelines, and instructions; These are updated routinely and whenever necessary;

w) The organisation works with risk-based access from DPIA and risk analyses;

x) The organisation submits itself to an external audit, ISAE3000, to demonstrate its adherence to the General Data Protection Regulation (GDPR). The report is available at the

end of each year starting in 2019; Controls are performed routinely and whenever necessary;

y) The organisation will work according to standard ISO27001 from 2020 onwards.

1.4 The following specific requirements apply to the Data Processor's erasure of personal data:

z) Web server logs are automatically erased after 30 days;

aa) Source files delivered by the client, and translations delivered by EasyTranslate can be erased permanently by the client upon conclusion of the order;

bb) Files on the platform can be automatically erased after a specific number of days according to an agreement between the client and EasyTranslate.

APPENDIX 3

PROOF OF OBSERVANCE

As part of the Data Controller's inspections of the Data Processor, the following points shall be executed and observed.

1 General Documentation for the Data Controller

1.1 The Data Processor shall forward the following general documentation to the Data Controller upon written request:

a) A declaration from the Data Processor's management that during processing of personal data on behalf of the Data Controller, the Data Processor regularly ensures observance of its contractual undertakings according to the Data Processing Agreement.

A description of the practical measures, including technical and organisational, the Data Processor has put into place to ensure observance of its contractual undertakings. The description can include a presentation of established and implemented management systems for information security, and for the processing of personal data, along with a description of measures put into place. The Data Processor shall also take part in follow-up meetings with the Data Controller as part of this process.

b) A description of which control precautions the Data Processor has put into place for the measurement and control of the effect of the management system for information security for the processing of personal data and result measurements from the same.

1.2 The general documentation shall be provided no later than five working days after a written request from the Data Controller, unless otherwise specifically agreed. The expense of compiling documentation shall be the sole responsibility of the Data Processor.

2 Auditor's declaration

2.1 When a general auditor's declaration exists or is compiled, the Data Processor shall annually and without separate payment submit the same concerning the level of its information security to the Data Controller.

2.2 When a general auditor's declaration exists or is compiled, the Data Processor shall annually and without separate payment submit the same concerning the level of its checks concerning data protection and the processing of personal data.

2.3 The auditor's declarations referred to in clauses 2.1 and 2.2 shall – unless otherwise agreed – be compiled according to generally accepted standards, such as ISAE 3000 type 1 or 2.

2.4 The audit declaration shall be compiled by a competent third party who shall be subject to the usual duty of confidentiality.

2.5 The audit declarations shall be submitted to the Data Controller immediately after the Data Processor has received them from an impartial third party.

2.6 The Data Processor shall commission the compilation and provision of additional auditor's declarations upon written request and for separate payment on aspects to be agreed in detail.

3 Physical meetings at the Data Processor's premises

3.1 The Data Processor shall take part in a physical meeting with the Data Controller at its own premises or those of the Data Controller, at which it shall be able to report on observance of the agreement and how such observance is ensured. A meeting request shall be given with at least 30 days' notice.

4 Audit

4.1 The Data Processor shall assist with access to an audit upon written request.

4.2 An audit shall be performed by an impartial third party chosen by the Data Controller and approved by the Data Processor. The Data Processor cannot reject a proposed third party without having reasonable grounds to do so. The impartial third party shall accede to a standard confidentiality declaration given to the Data Processor. An audit request shall be given with at least 30 days' notice. Some details will be kept confidential, e.g. code, personal data and any test results.

5 Miscellaneous

5.1 The above clauses cannot be regarded as exhaustive, and the Data Processor shall therefore undertake such additional actions and measures deemed necessary to demonstrate compliance with its undertakings according to clause 4 of the Data Processing Agreement.

5.2 The Data Processor is not obliged to follow a recommendation from the Data Processor according to Appendix 3 if that recommendation contravenes personal data regulations. The Data Processor shall inform the Data Controller when this is deemed to be the case.

APPENDIX 5

THE DATA CONTROLLER'S

UNDERTAKINGS

1 Undertakings

1.1 The Data Controller has the following undertakings

1.1.1 The Data Controller is responsible for compliance with data protection legislation with regard to the personal data passed to the Data Processor for processing. The Data Controller is specifically responsible for ensuring that:

- The Data Processor can act in accordance with Appendix 1, including with regard to establishing the necessary security precautions.
- The Data Controller has the necessary legal grounds to process and to pass the personal data to be processed to the Data Processor in connection with provision of the Principle Services.
- The Instructions given, in accordance with which the Data Processor shall process the personal data on behalf of the Data Controller, are legal.
- Anonymising of personal data where relevant

1.1.2 The Data Controller shall inform the Data Processor in writing of any consequence analyses performed that are relevant to the processing activities, and the Data Controller shall also give the Data Processor insight into such analyses with regard to the Data Processor being able to fulfil its contractual undertakings according to the Data Processing Agreement.

1.1.3 The Data Controller shall also inform the Data Processor of any matters of importance to the latter's performance of its undertakings according to the Data Processing Agreement, including the Data Controller's regular risk assessment to the extent relevant to the Data Processor.

1.1.4 The Data Controller shall also inform the Data Processor if the applicable data protection law with regard to the personal data passed to the Data Processor for processing covers anything other than the Data Protection Act, or Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.1.5 The Data Controller shall assist the Data Processor to enter into agreements with Sub-Data Processors to the extent necessary, including to ensure the legal grounds for transfer to Third Countries

APPENDIX 6

SUB-DATA PROCESSORS

1 General information

1.1 The Data Controller hereby gives its consent to the Data Processor using the following Sub-Data Processors:

https://www.easytranslate.com/en/dpa-vendors/

1.2 The Data Controller hereby gives its prior general written consent to the Data Processor using a Sub-Data Processor. The Data Processor shall inform the Data Controller in writing of the addition or replacement of a Sub-Data Processor prior to starting to use the same. This shall be performed via the above link, and the Data Controller shall receive a notification whenever the content of the list changes. Correspondingly, the Data Processor shall inform the Data Controller when ceasing to use a Sub-Data Processor.

1.3 The Data Controller can object to such a Sub-Data Processor when there are reasonable grounds for doing so.

2 SPECIAL TERMS AND CONDITIONS

2.1 The following Sub-Data Processors will be used for processing on the following special terms and conditions, which take preference over this Data Processing Agreement:

Sub-Data Processor	Terms and conditions
DreamData, Købmagergade 22, 2.2., 1150 Copenhagen K, VAT: 39855224	Not yet certified but working towards ISO27001
Dixa, Vimmelskaftet 41 A, 1., 1161 København K	Not yet audited externally, but will be by 2020

APPENDIX 7

TRANSFER TO THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

1 General information

1.1 The Data Controller hereby gives its prior general written consent to the Data Processor transferring personal data to a Third Country, or international organisation. The Data Processor shall inform the Data Controller in writing prior to transfer to a new Third Country or international organisation. Correspondingly, the Data Processor shall inform the Data Controller when ceasing to do so. This shall be performed via the below link, and the Data Controller shall receive a notification whenever the content of the list changes.

https://www.easytranslate.com/en/dpa-vendors/

1.2 The Data Controller can object to such a transfer when there are reasonable grounds for doing so.