Data Processing Agreement in Accordance with Article 28 of the General Data Protection Regulation (GDPR)

Agreement

between

- the Controller - hereafter named the "**Client**" -

and

Weblate s.r.o., ID: 21668027, with its registered office at Nábřežní 694, Cvikov II, 471 54 Cvikov, Czechia, registered in the Commercial Register kept at the Regional Court in Ústí nad Labem, file no. C 52324

- the Processor - hereafter named the "**Supplier**" -

1. Subject matter and duration of the Agreement or Contract

The subject matter and duration of the agreement (hereafter named “**Agreement**”) shall be determined entirely according to the information provided in the contract concluded by and between the Parties for the provision of Weblate services (hereafter referred to as “**Contract**”).

The Supplier shall process personal data for the Client in accordance with Art. 4 No. 2 and Art. 28 GDPR on the basis of this Agreement.

2. Object, nature, and purpose of the collection, processing or use of data

The object, nature and purpose of any possible collection, processing, or use of personal data, the nature of data, and the Affected People (as defined below) shall be described to the Supplier by the Client in accordance with Appendix 1 of this document as completed by the Client, insofar as this is not governed by the Agreement described the content of Section 1 of this document.

The provision of the contractually agreed upon data processing shall occur exclusively in a member state of the European Union or in another member state party to the Agreement on the European Economic Area. Any transfer to a third country shall require the prior consent of the Client and may only occur if the special conditions defined in Articles 44 et seq. of the GDPR are fulfilled.

3. Technical and organizational measures in accordance to Art. 32 GDPR (Art. 28 Para. 3 Sent. 2 Clause c of the GDPR)

1. Before the commencement of data processing, the Supplier shall document the execution of the necessary Technical and organizational measures defined in advance of the execution of the Contract, specifically with regard to the detailed execution of the Agreement or Contract, and shall present these documented measures to the Client for inspection (See Appendix 2 of this document). Upon acceptance of said documents by the Client, the documented measures become the foundation of the this Agreement. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

2. The Supplier shall establish the security of the data in accordance with Art. 28 Para. 3 Sent. 2 Clause c, and Art. 32 GDPR in particular in conjunction with Art. 5 Para. 1 and Para. 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the technology; implementation costs; the nature, scope, and purposes of processing; as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the scope of Art. 32 Para. 1 GDPR must be taken into account.

3. The technical and organizational measures shall be subject to technical progress and further development. In this respect, the Supplier is permitted to implement alternative adequate measures. The safety level of the specified measures must not be compromised. Substantial changes shall be documented.

4. Correction, restriction, and deletion of data

1. The Supplier is not entitled of his own authority to delete or restrict the processing of data processed on behalf of third parties. Insofar as an Affected Person contacts the Supplier directly in this respect, the Supplier will immediately forward this request to the Client without delay.

2. Insofar as the scope of services under the Contract and this Agreement includes, the following are to be ensured without undue delay by the Supplier in accordance with the Client's documented instructions: a deletion policy, the "right to be forgotten", data correction, data portability, and data disclosure. However, the Supplier may claim compensation for such services provided to the Client on the basis of hourly rate as stipulated in Article 11.1 of this Agreement.

5. Quality assurance and other duties of the Supplier

In addition to complying with the provisions of this Agreement, the Supplier shall comply with statutory obligations in accordance with Articles 28 to 33 GDPR; in this respect, the Supplier shall particularly ensure compliance with the following requirements:

- Benjamin Alan Jamie (privacy@weblate.org) is appointed to the role of Data Protection Officer by the Supplier. The Client shall be immediately notified of any change of the Data Protection Officer. The Data Protection Officer's current contact details are easily accessible on the Supplier's website.
- Confidentiality in accordance with Art. 28 Para. 3 Sent. 2 Clause b, Art. 29 and Art. 32 Para. 4 GDPR. The Supplier entrusts only such employees or subcontractors with the data processing defined in this Agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data may only process that data in accordance with the instructions of the Client (which includes the powers granted in this Agreement) unless otherwise required to do so by law.
- The implementation and observance of all technical and organizational measures necessary for this Agreement in accordance with Art. 28 Para. 3 Sent. 2 Claus c, Art. 32 GDPR are specified in Appendix 2 of this Agreement.
- The Supplier and the Client shall, upon request, cooperate with the supervisory authority in the performance of their duties.
- The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Agreement or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, administrative rule, or regulation regarding the processing of personal data in connection with the processing of this Agreement or Contract.
- Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim of an Affected Person or a third party or any other claim in connection with the processing of the Agreement or Contract by the Supplier, the Supplier shall make reasonable effort to support the Client in such inspection provided that adequate reimbursement of costs to the Supplier is provided.
- The Supplier shall regularly monitor the internal processes as well as the Technical and organizational measures to ensure that the processing in his area of responsibility is executed in accordance with the requirements of the applicable data protection law and that the rights of the Affected People are protected.

6. Subcontractors

For the purposes of this Agreement, subcontracting relationships are defined as those services which relate directly to the provision of the principal commission. This does not include ancillary services which the Supplier uses, e.g. telecommunications services; postal/transport services; maintenance and user support services; as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Supplier is obligated to make appropriate and legally binding contractual arrangements and implement appropriate inspection measures to guarantee data protection and data security of the Client's data, even in the case of outsourced ancillary services. An up to date list of the subcontractors can be found at: https://hosted.weblate.org/legal/contracts/.

7. The Client’s inspection rights

1. The Client shall have the right to implement inspections in consultation with the Supplier or to have them implemented by inspectors designated in individual cases. The Client shall have the right to verify compliance with this Agreement by the Supplier in his business operations by means of spot inspections, which shall as a general rule be announced at least 10 business days prior to any planned inspection.

2. The Supplier shall ensure that the Client can verify the Supplier's compliance with the obligations under Article 28 of the GDPR. The Supplier is obligated to provide the Client with the necessary information upon request and in particular to provide proof of the implementation of the Technical and organizational measures.

3. Evidence of such measures which concern not only this specific Agreement or Contract may be provided by compliance with approved codes of conduct pursuant to Article 40 GDPR; certification according to an approved certification procedure in accordance with Article 42 GDPR; current auditor’s certificates, reports, or excerpts from reports provided by independent bodies (e.g. an auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor); or a suitable certification by IT security or data protection auditing. The Client, however, acknowledges that the Supplier does not implement any approved codes of conduct within the meaning of Article 40 GDPR at the time of conclusion of the Agreement.

4. The Supplier may assert a claim for remuneration for enabling the Client’s inspections as is described below.

8. Cooperation by the Supplier and Liability of the Supplier

1. The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments, and prior consultations referred to in Articles 32 to 36 of the GDPR. These include:

    a) Ensuring an adequate level of protection with the Technical and organizational measures that take into account the circumstances and purposes of the data processing, the projected probability and severity of potential breaches of the law due to security vulnerabilities, and measures that enable relevant breaches of the law to be detected immediately.
    b) The obligation to immediately report violations of personal data to the Client.
    c) The duty to assist the Client with regard to the Client's own obligation to provide information to the Affected People and, in this context, to immediately inform the Client of its own obligations.
    d) Assisting the Client with his data protection impact assessment.
    e) Assisting the Client with regard to prior consultation with the supervisory authority.

2. The Supplier may claim compensation for support services which are not included in the description of the services provided to the Client under the Contract and/or Agreement and which are not attributable to failures on the part of the Supplier.

3. The Supplier shall not be liable for any direct, indirect, incidental, consequential, special, exemplary, or punitive damages, including but not limited to loss of profits, revenue, business opportunities, goodwill, or data, arising out of or in connection with the processing of personal data under this Agreement, except to the extent that such damages are the direct result of the Supplier's gross negligence or wilful misconduct.

4. The Supplier shall not be liable for any damages or claims brought against the Client by any third parties, including data subjects, sub-processors, employees, or other entities engaged by the Supplier in the course of providing services, except to the extent that such damages are directly caused by the Supplier's gross negligence or wilful misconduct.

5. The Supplier shall not be liable for any acts or omissions of sub-processors or other third parties engaged in the processing of personal data on behalf of the Supplier, unless such acts or omissions are a direct result of the Supplier's gross negligence or wilful misconduct.

6. The Supplier shall not be liable for any failure to perform its obligations under this Agreement if such failure results from circumstances beyond its reasonable control, including but not limited to natural disasters, acts of God, war, terrorism, strikes, lockouts, labor disputes, governmental regulations, or any other events that are not attributable to the Supplier's gross negligence or wilful misconduct.

7. In no event shall the Supplier's aggregate liability arising out of or in connection with this Agreement exceed the total amount paid by the Client to the Supplier for the services rendered under the Contract in the twelve (12) months preceding the event giving rise to the claim.

8. The Client agrees to indemnify, defend, and hold harmless the Supplier from and against any and all claims, liabilities, damages, losses, and expenses, including reasonable attorneys' fees, arising out of or in any way connected with:

    a) The Client's use of the Supplier's services.
    b) The Client's breach of this Agreement.
    c) Any data processing instructions given by the Client to the Supplier.
    d) The Client's violation of applicable data protection laws.

9. The Client's authority to issue instructions

1. The Client shall immediately confirm any oral instructions provided to the Supplier in the text form, in the minimum via e-mail sent to the Supplier.

2. The Supplier shall inform the Client immediately if he believes that an instruction violates data protection regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or alters said instructions.

3. The Client acknowledges and agrees that the Supplier's liability is strictly limited to the actions directly attributable to the Supplier's own conduct. The Supplier shall not be liable for any damages resulting from:

    a) The Client's instructions or failure to provide adequate instructions.
    b) The Client's breach of its own obligations under applicable data protection laws.
    c) Any actions or inactions of the Client's employees, agents, or other representatives.
    d) Any actions or inactions of the Client's sub-contractors or partners.

10. Deletion and return of personal data

1. Copies or duplicates of the data shall not be created without the knowledge of the Client, with the exception of backup copies as far as they are necessary to ensure proper data processing as well as data required for compliance with statutory storage obligations.

2. After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Contract, the Supplier shall submit to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the Contract that have come into its possession in accordance with

data protection law. The same applies to any and all connected test and scrap material. Upon request, the Supplier shall provide the Client with information on nature and the time of the data's deletion.

3. The Supplier shall retain documentation that proves that data was processed in an orderly and contractual manner after the respective Contract period has elapsed in accordance with respective retention periods beyond the end of the Contract and/or this Agreement. Alternatively, the Supplier may be absolved of this duty by transferring said documentation to the Client upon the termination of the Contract and/or this Agreement.

11. Other agreements

11.1. Reimbursement

- No additional fee for this Agreement shall be granted to the Supplier as it was already provided for within the Contract for the baseline obligations under this Agreement. However, the Supplier shall be reimbursed for any costs and expenses incurred with the following:
  - If the Client requires assistance in answering inquiries from Affected People as described in section 4 and 5 of this Agreement, the Client shall be required to reimburse all expenses of the Supplier incurred by the Supplier as a result of such assistance.
  - If the Client exercises monitoring rights as described in section 7 and 8 of this Agreement, the amount of remuneration to be agreed upon will be based on the fixed hourly rate of the Supplier's employee who is instructed to supervise the auditor. If no fixed hourly rate is agreed in the Contract, such hourly rate shall be EUR 80.
  - If the Client issues instructions to the Supplier as described in section 9 of this Agreement, the Client shall be required to pay any expenses incurred to the Supplier as a result from these instructions.
- Unless otherwise agreed in this Agreement the reimbursement of any expenses incurred by the Supplier shall be remunerated on an hourly high-watermark basis while the hourly rate is stipulated in the Price List found at https://weblate.org/support/.

11.2. Duration of the Agreement

This Agreement is dependent on the existence of a Contract as described in section 1 of this Agreement. The cancellation or other termination of the Contract as described in section 1 shall simultaneously terminate this Agreement.

The right to unilateral termination or withdrawal of this Agreement by a written notice of termination or withdrawal hereby remains intact as guaranteed by the statutory obligations provided in the laws of the Czech Republic.

11.3. Choice of law

The laws of the Czech Republic shall apply.

11.4. Place of jurisdiction

The Parties agree that the place of jurisdiction shall be the general court of the Supplier, as stipulated under Act No. 99/1963 Coll., Code of Civil Procedure, as of the day of the conclusion of this Agreement.

Signatures

_____, date _____

_____ _____

Client Supplier

Appendix 1 Pursuant to Art. 28 GDPR: List of Personal Data and the Purpose of Their Being Processed

1. Types of data

The following types and categories of data are the object of this Agreement:

- Personal identification data
- Communication data (e. g. telephone, email)
- Contractual master data
- Log data

2. Affected People

Those affected as a result of this Agreement include:

- The Client's customers, contractors and employees

Appendix 2 of the Agreement Pursuant to Art. 28 GDPR: Technical and Organizational Measures in Accordance with Art. 32 GDPR and Amendments

1. Confidentiality

- Physical access control
  - Secure data centers are provided by a subcontractor (mainly company Hetzner Online GmbH) and located in EU. An up to date list of the subcontractors can be found at: https://hosted.weblate.org/legal/contracts/
- Electronic access control
  - for dedicated and hosted servers
    - Access is password-protected and only employees of the Supplier have access to the passwords. Passwords must meet a minimum length, and new passwords shall be changed on a regular basis.
  - for self-hosted servers
    - The responsibility for access control is incumbent upon the Client.
    - Access is granted to the Supplier and the Supplier is responsible for securing the granted access credentials.
- Internal access control
  - for the Supplier's internal administration systems
    - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
    - a revision-proof, compulsory process for allocating authorization for Supplier employees
  - for dedicated and hosted servers
    - The Supplier shall prevent unauthorized access by applying security updates regularly by using state of the art technology.
    - a revision-proof, compulsory process for allocating authorization for Supplier employees
  - for self-hosted servers
    - The responsibility for access control is incumbent solely upon the Client.

- Transfer control
  - Drives that were in operation on cancelled servers will be swiped multiple times (deleted) in accordance with data protection polices upon termination of the contract. After thorough testing, the swiped drives will be reused.
  - Defective drives that cannot be securely deleted shall be destroyed (shredded).
- Isolation control
  - for the Supplier's internal administration systems
    - Data shall be physically or logically isolated and saved separately from other data.
    - Backups of data shall also be performed using a similar system of physical or logical isolation.
  - for dedicated and hosted servers
    - Data shall be physically or logically isolated and saved separately from other data.
    - Backups of data shall also be performed using a similar system of physical or logical isolation.
  - for self-hosted servers
    - The Client is solely responsible for isolation control.
- Pseudonymization and Anonymization
  - The Client is solely responsible for pseudonymization and anonymization, if applicable.

2. Integrity (Art. 32 Para.1 Clause b GDPR)

- Data transfer control
  - All employees and subcontractors are trained in accordance with Art. 32 Para. 4 GDPR and are obliged to ensure that personal data is handled in accordance with data protection regulations.
  - Deletion of data in accordance with data protection regulations after termination of the Contract and/or Agreement.
  - Encrypted data transmission options are provided within the scope of the service description of the principal commission.
- Data entry control
  - Data is entered or collected by the Client.

3. Availability and Resilience (Art. 32 Para. 1 Clause b GDPR)

- Availability control
  - for the Supplier's internal administration systems
    - backup and recovery concept with daily backups of all relevant data
    - professional employment of security programs (virus scanners, firewalls, encryption programs, spam filters)
    - employment of disk mirroring on all relevant servers
    - monitoring of all relevant servers
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for dedicated and hosted servers
    - backup and recovery concept with daily backups of all relevant data
    - professional employment of security programs (virus scanners, firewalls, encryption programs, spam filters)
    - employment of disk mirroring on all relevant servers
    - monitoring of all relevant servers
    - employment of an uninterruptible power supply system or emergency power supply system
    - permanently active DDoS protection
  - for self-hosted servers
    - Data backup is incumbent solely upon the Client, it can be provided as an additional service by the Provider for a fee, if explicitly agreed upon in the Contract.
    - Data protection and system monitoring is incumbent solely upon the Client.
  - Rapid recovery measures (Art. 32 Para. 1 Clause c GDPR)
    - For all internal systems, there is a defined escalation chain which specifies who is to be informed in the event of an error in order to restore the system as quickly as possible.

4. Procedures for regular testing, assessment, and evaluation (Art. 32 Para. 1 Clause d GDPR; Art. 25 Para. 1 GDPR)

- The data protection management system and the information security management system have been combined into a DIMS (data protection information security management system).
- Incident response management is available.
- Data-protection-friendly default settings are taken into account for software development (Art. 25 Para. 2 GDPR).
- Agreement or Contract control
    - All employees are regularly instructed in data protection laws and are familiar with the procedural instructions and user guidelines for data processing on behalf of the Client also with regard to the Client's right of instruction. The Contract (incorporation General Terms and Conditions) contains detailed information on the type and scope of the commissioned data processing and use of the Client's personal data and about the purpose limitation of Client’s personal data.
    - The data protection organization and the information security management systems are integrated into the relevant operational procedures.