Data Processing Addendum ("Addendum")

Between _____("Company)
and
Crowdin OÜ ("**Crowdin**")
(Company and Crowdin also referred to as a "Party" and collectively as the "Parties")

1. Background

The Parties have agreed to the Terms of Service posted at https://support.crowdin.com/terms/ ("Framework Agreement") according to which Crowdin has agreed to provide certain services to Company (hereinafter the "Services").

When providing the Services, Crowdin may collect, process and gain access to personal data of individuals on behalf of Company. From a data protection perspective, Company will be the data controller and Crowdin will be the data processor.

This Data Processing Addendum specifies the data protection obligations of the Parties under the Framework Agreement. It applies to all activities performed by Crowdin in connection with the Framework Agreement in which Crowdin, its staff or a third party acting on behalf of Crowdin comes into contact with personal data of individuals.

If there is a conflict between the terms of the Framework Agreement and those of this Data Processing Addendum, the provisions of this Addendum will prevail.

2. Crowdin's Obligations

2.1 Crowdin will collect and process personal data in connection with the Framework Agreement only for the purpose of fulfilling the Framework Agreement. Crowdin will carry out the data processing operations in accordance with the Framework Agreement as well as any written instructions received from Company that do not conflict with the provisions of this Data Processing Addendum or the Framework Agreement.

2.2 Personal data to which Crowdin may receive access concern the following data subjects ("Data Subjects"):

2.2.1 Company's directors, officers, employees, interns, trainees, agents, contractors, job applicants, customers, suppliers, subcontractors, business contacts;

2.2.2 Company's customers' directors, officers, employees, interns, trainees, agents, contractors, customers or business contracts;

2.2.3 Any third party with whom Crowdin interacts or is requested to interact in connection with the provision, operation, or maintenance of the Services on behalf of Company:

2.2.4 Any other individuals for which Company enters personal data or information into the Service.

Crowdin will not have any knowledge or control over the categories or identities of the Data Subjects whose Personal Data Company may elect to record or upload into the Service, except as provided in the Framework Agreement.

2.3 The data processing activities will generally include the following categories of personal data ("Personal Data"):

2.3.1 Name, email address, other contact information, company name, title;

2.3.2 Customer history;

2.3.3 IP Addresses;

2.3.4 References, comments, discussions, localization and context resources; and

2.3.5 Such categories of personal data pertaining to an identified or identifiable individual as Company or Company's representative may enter or upload from time to time into the Service.

Crowdin will not have any knowledge or control over the categories or nature of the Personal Data that Company may elect to record or upload into the Service, except as provided in the Framework Agreement.

2.4 Crowdin will not collect, process or use any Personal Data made available to it for any purposes other than for the performance of the Services. Copies or duplicates of any Personal Data made available hereunder may only be compiled with the approval of Company or as permitted under the Framework Agreement.

2.5 Crowdin will grant to Company and its designees during the term of the Data Processing Addendum all requested information and access rights strictly in accordance with Crowdin's security policy in order to verify Crowdin's compliance with the Framework Agreement, this Data Processing Addendum and with applicable data protection law.

Company may determine Crowdin's compliance with the agreed technical and organizational measures (see **Exhibit 1** of this Data Processing Addendum) at Crowdin's facilities. If and to the extent Company engages third parties to conduct the audit, such third parties have to be bound to confidentiality obligations similar to those agreed for Crowdin under this Data Processing Addendum.

2.6 Crowdin will notify Company without undue delay if Crowdin is of the opinion that a written instruction received from Company is in violation of applicable data protection law and/or in violation of contractual duties under the Framework Agreement.

2.7 Crowdin will notify Company without undue delay if Crowdin becomes aware that Crowdin's employees have violated any data protection law, or the provisions of the Framework Agreement if the violation occurs in the course of the processing of the data by Crowdin. Furthermore, if Crowdin is of the opinion that personal Data have been or might have been illegally transferred or otherwise illegally disclosed to or accessed by a third party, Crowdin will notify Company thereof without undue delay in accordance with applicable data protection laws, in particular Regulation (EU) 2016/679. In case of any loss of, or unauthorized access to Personal Data stored on the Service, Crowdin will inform Company without undue delay, and assist Company in fulfilling its statutory obligations under applicable data protection laws, in particular Regulation (EU) 2016/679.

2.8 Company grants Crowdin a general authorization in the meaning of Article 28 (2) of Regulation (EU) 2016/679 to engage processors for the purposes of providing the Crowdin Services. Crowdin will inform Company of changes in such processors in the Framework Agreement in accordance with the procedure of modifying the Framework Agreement.

2.9 Crowdin may only engage Subcontractors for providing the Services under the Framework Agreement if Crowdin (i) communicates the name, address and contact details of the subcontractor and the tasks of the subcontractor prior to engaging the subcontractor, (ii) has in place or concludes prior to engaging the subcontractor a sub-processing agreement between Crowdin and the subcontractor that is no less protective with respect to Company's interest and protection of Personal Data than this Data Processing Addendum, (iii) ensures that an adequate level of data protection for subcontractors that are located outside of the EU/EEA exists or is created (e.g. by concluding EU Standard Contractual Clauses or by selecting subcontractors that are certified under the Privacy Shield framework) (iv) has sufficient rights against the subcontractor to enforce a claim or request of Company in context of the Services provided by the subcontractor and (v) provides copies of documentation evidencing (ii) to (iv) above before engaging the subcontractor.
2.10 Crowdin will use only Subprocessors that have executed written contracts with Crowdin containing obligations that are substantially similar to those of Crowdin under this DPA. Crowdin will be liable for the acts and omissions of its Subprocessors to the same extent Crowdin would be liable if performing the services of each Subprocessor directly under the terms of this DPA.
2.12 Crowdin will keep confidential and will not make available any Personal Data received in connection with the Framework Agreement to any third party except as required by applicable law;
2.12 Crowdin will support Company in fulfilling the rights of the Data Subject, in particular with regard to correction, blocking, deletion, and provision of Personal Data. If so instructed by Company, and if feasible, Crowdin will correct, block or delete Personal Data in accordance with Company's written instructions. If a Data Subject contacts Crowdin directly in order to have his or her data corrected, deleted or blocked, Crowdin will forward such request to Company without undue delay after receipt of such request.
2.13 Crowdin will adopt adequate technical and organizational measures to ensure security of its network and data centre operations for the purposes of providing the Services to Company in accordance with **Exhibit 1**.
2.14 Crowdin will use reasonable efforts to fully cooperate and to comply with any instructions, guidelines and orders received from the relevant supervisory authority when such instructions, guidelines or orders pertain to the Personal Data.
2.15 Upon termination of the Framework Agreement or, if applicable, an agreed exit phase, upon written instruction from Company, Crowdin will return all media provided by Company with regard to the Framework Agreement containing Personal Data and will destroy any other Personal Data within 3 months of termination of the Framework Agreement.
2.16 Crowdin and each its Affiliate shall provide reasonable assistance to each Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available.

3. Obligations of Company

3.1 Company will be responsible for the evaluation of the admissibility of the data processing and for ensuring the rights of the data subjects concerned.

3.2 Company will be entitled to issue written instructions regarding the scope and the procedure of the data processing.

4. Personnel

4.1 Crowdin will be use qualified personnel with data protection training to provide the Services.

4.2 Crowdin will oblige its employees to process and use the Personal Data only in accordance with the Framework Agreement, this Data Processing Agreement, including its exhibits, and any written instructions received from Company.

4.3. Crowdin ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Crowdin takes all measures required pursuant to Article 32 of Regulation (EU) 2016/679.

5. Technical and Organizational Measures

Crowdin will implement the technical and organizational security measures as set forth in **Exhibit 1** to this Data Processing Addendum. The technical and organizational security measures will be aimed at protecting the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. Upon Company's request, but not more frequently than once in any twelve (12) month period, Crowdin will provide a self-audit report or a third-party report confirming compliance with the technical and organizational security measures before processing or accessing any Personal Data on behalf of Company.

6. Term

This Data Processing Addendum will become effective when signed by the Parties ("**Effective Date**"). It will run for the same term as the Framework Agreement.

7. Choice of Law

The Data Processing Addendum is governed by the law indicated as the governing law in the respective provisions of the Framework Agreement.

Company: _____	Company: **Crowdin OÜ**
Name: _____	Name: **Serhiy Dmytryshyn**
Position: _____	Position: **Executive Manager**
Date: _____	Date: November 1, 2018
Signature: _____	Signature: _____

EXHIBIT 1 to Data Processing Addendum

Technical and Organizational Measures
Description of the technical and organizational security measures implemented by Crowdin according to Sec. 5 of the Data Processing Addendum:

1. Access Control of Processing Areas

Crowdin will implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers and related hardware) where the Personal Data are processed or used. This will be accomplished by:

- establishing security areas;
- protection and restriction of access paths;
- securing the decentralized data processing equipment and personal computers;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data centre where personal data are hosted is logged, monitored, and tracked;
- the data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

2. Access Control to Data Processing Systems

Crowdin will implement suitable measures to prevent its data processing systems from being used by unauthorized persons. This will be accomplished by:

- identification of the terminal user to the data importers systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered, log file of events, (monitoring of break-in-attempts);

3. Access Control to Use Specific Areas of Data Processing Systems

Crowdin will ensure that the persons entitled to use the Crowdin data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization). Crowdin will ensure that Personal Data cannot be read, copied or modified or removed without authorization. This will be accomplished by:

- employee policies and training in respect of each employee's access rights to the personal data;
- effective and measured disciplinary action against individuals who access personal data without authorization;
- release of data to only authorized persons;
- control of files, controlled and documented destruction of data; and
- policies controlling the retention of back-up copies.

4. Transmission Control

Crowdin will implement suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data. This will be accomplished by:

- use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

5. Input Control

Crowdin will implement suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This will be accomplished by:

- an authorization policy for the input of data into memory, as well as for the reading, alteration and deletion of stored data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of user codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within data importers' organization of the input authorization;

6. Job Control

Crowdin will implement suitable measures to ensure that the Personal Data are processed strictly in accordance with the instructions of Company. This will be accomplished by:

- ensuring clear instructions to Crowdin regarding the scope of any processing of Personal Data. This will be limited to specific system development and database management requirements of Company; and
- granting regular access and control rights to Company, on appropriate notice and in accordance with Company's security policies and accompanied by Crowdin.

7. Availability Control

Crowdin will implement suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This will be accomplished by:

- infrastructure redundancy: two clustered database servers will be used for storing the data;
- backup is stored at dedicated server, closed inside the infrastructure and available for restore in case of failure of database server.

8. Separation of Processing for different Purposes

Crowdin will implement suitable measures to ensure that data collected for different purposes can be processed separately. This will be accomplished by:

- access to data will be separated through application security for the appropriate users;
- modules within Crowdin's database will separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data will be stored in different normalized tables, separated per module or function they support; and
- interfaces, batch processes and reports will be designed for only specific purposes and functions, so data collected for specific purposes is processed separately.