Semantix

Appendix 1A

This Data Processing Appendix (this "Appendix") is incorporated into the Service Agreement (the "Agreement") executed between the Customer (the "Purchaser") and Semantix (the "Supplier"), together the "Parties".

1.   DEFINITIONS

"Controller" shall mean the entity which determines the purposes and means of the processing of Personal Data.

"Processor" shall mean the entity which processes Personal Data on behalf of the Controller.

"Data Subject" shall mean an identified or identifiable natural person; an identified or identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

"Third Party" shall mean a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.

"Laws" shall mean applicable laws relating to data protection, privacy and security, including without limitation EU Directive 95/46/EC EU and Directive 2002/58/EC (collectively the "EU Directives") and any amendments, replacements or renewals thereof, including but not limited to EU General Data Protection Regulation 2016/679, as well as all binding national laws implementing the EU Directives and other applicable binding data protection, privacy or data security directives, laws, regulations and rulings when processing Personal Data under the Agreement.

"Model Clauses" shall mean the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the transfer of Personal Data to Processors established in third countries under the EU Directives and any amendment, replacement or renewal thereof by the European Commission.

"Personal Data" shall mean any information relating to a Data Subject which is sent to the Supplier, is accessed by the Supplier or is otherwise processed by the Supplier on Purchaser's behalf in relation to the Services.

"Personal Data Breach" shall mean breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Processing" shall mean any operation whereby the Supplier or its affiliates or subcontractors process Personal Data, such as collection, recording, storage, combining, organisation, alteration, calculation, analysis, use, disclosure by transmission, dissemination, erasure or deletion.

"Services" shall mean the provision of the services by Supplier to Purchaser under the Agreement.

"Technical and organisational security measures" shall mean those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss,

Semantix

alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. PROCESSING OF PERSONAL DATA

2.1. Role of the Parties

The Parties acknowledge and agree that with regard to the Processing of Personal Data under this Appendix, Purchaser is a Controller and Supplier is a Processor.

2.2. Processing of Personal Data

Supplier agrees to comply with the provisions of all Laws applicable to the Processing of Personal Data. Supplier shall (and shall procure that any subcontractor shall) also comply with written instructions of Purchaser or data protection authorities provided to Supplier, e.g. on handling, protecting and encrypting Personal Data. Supplier will comply with all such instructions without additional charge to the extent necessary for Purchaser or Supplier to comply with the Laws. Supplier shall also assist Purchaser at Purchaser's reasonable request in conducting impact assessments for the Processing activities and in consulting the supervisory authorities prior to Processing when the impact assessment indicates a high risk. In the event the Supplier believes that the Supplier does not have sufficient instructions or other information in respect of how the processing of Personal Data on behalf of the Purchaser is to take place, the Supplier shall ensure that any such instruction or information is obtained from the Purchaser.

Except to the extent required by applicable legislation, Supplier shall not use or process Personal Data for any purpose, except as defined or instructed by Purchaser. Supplier shall keep Personal Data confidential and shall have no rights to Personal Data. Supplier shall not, during or after the term of the Agreement, disclose or transfer, or enable access to or processing of, Personal Data to or by any Third Party other than as agreed with Purchaser. For the avoidance of doubt, transfers of Personal Data to subcontractors approved by Purchaser for the purposes of this agreement are permitted. Supplier shall not disclose or use data derived from Personal Data for its own purposes.

2.3. Use of subcontractors

The Purchaser authorises the Supplier to engage subcontractors to assist in the provision of the Services. The approved categories of subcontractors engaged in processing Personal Data and the approved subcontractors for processing Personal Data in systems are described in Annex 2. The Supplier will inform the Purchaser of any new or change of subcontractors.

The engagement of subcontractors will be under a written contract and will require the subcontractor to comply at the minimum level with the same obligations applicable to Supplier under this Appendix and the Laws. In any event, Supplier covenants to Purchaser that Supplier will remain fully liable for the acts and omissions of its subcontractors.

2.4. Data deletion at termination or expiry of Agreement

Upon termination or expiry of the Agreement or Services, Supplier shall (and shall procure that its subcontractors shall) return to Purchaser all data, and then destroy any Personal Data from all computer hardware (including storage media), software, and databases used by Supplier to process the Personal Data, and shall confirm in writing that this has been done.

Semantix

2.5. Data disclosures

Any requests from governmental authorities regarding access to Purchaser's Personal Data that the Supplier may receive should be immediately notified to Purchaser, unless such notification is prohibited by applicable law. Supplier should not respond to such a request without Purchaser's prior written approval.

3. TRANSFER OF PERSONAL DATA

The Purchaser authorises the Supplier to transfer personal data to a third country, i.e. a country outside the EU/EEA. Supplier will be required to ensure that such transfer is at all times lawful, e.g. by ensuring that Model Clauses, or a similar legal safeguard approved by Laws, will apply to such transfer.

If required by the Laws, Supplier shall (and shall procure that any subcontractors shall) enter into the appropriate Model Clauses. For the avoidance of doubt, the Supplier shall not be obliged to enter into Model Clauses if the transfer is subject to other applicable safeguards, such as an adequacy decision, other appropriate safeguards including BCRs, the data subject's consent or if needed for performance of a contract with the data subject. The unchanged version of the Model Clauses shall be deemed incorporated by reference hereto as Annex 3, and shall apply if the Supplier or its subcontractor can either (a) remotely access Personal Data hosted in a data center in the EU/EEA from a non-EU/EEA country, or (b) transfer to, or process data hosted in, a non-EU/EEA country. In the event of any conflict or inconsistency between this Data Processing Appendix and the Model Clauses, the Model Clauses shall prevail; provided that (i) the Model Clauses offers a higher level of protection for Personal Data, or (ii) the Laws require the Model Clauses to be applied.

The Purchaser grants a power of attorney to the Supplier to represent the Purchaser in signing the Model Clauses on behalf of the Purchaser. Furthermore, Purchaser explicitly accepts that Supplier may also represent the subcontractor in question in relation to the Model Clauses.

4. DATA SECURITY AND SAFEGUARDS

Supplier shall implement and maintain at all times appropriate organisational, operational, managerial, physical and technical measures to protect the Personal Data and Purchaser's any other data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access, so that all processing is in compliance with the Laws and Purchaser's reasonable written instructions, especially where the processing involves the transmission of data over a network. These measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

Technical safeguards shall include all technical security controls defined by Supplier, following the recommendations as laid out in ISO/IEC 27000 series (or equivalent, such as SSAE-16(2)) or other recommendations adapted to a level which is suitable, taking into consideration the degree of sensitivity of the personal data, the particular risks which exist, existing technical possibilities, and the costs for carrying out the measures. Supplier shall limit access to the Personal Data to authorised and properly trained personnel with a well-defined "need-to-know" basis, and who are bound by appropriate confidentiality obligations. Supplier shall also ensure by technical and organisational means that Purchaser's Personal Data is not processed for different purposes (e.g. for different Supplier customers) and that the Personal Data is processed separately from the data of other Supplier customers.

Semantix

Supplier warrants that in performing the Services under the Agreement all necessary precautions are taken by Supplier to prevent loss and alteration of any data, to prevent unauthorised access to Purchaser's IT environment, to prevent introduction of viruses to Purchaser's systems, and to prevent improper access to Purchaser's IT environment and confidential information of Purchaser.

5. SELF-ASSESSMENTS AND AUDITS

On a semi-annual basis during the term of the Agreement Purchaser may request a review of Supplier's security documentation and/or a written report of self-assessment on Supplier's compliance with this Appendix, the Agreement and the Laws.

In addition, Purchaser (or an independent Third Party on its behalf) may audit the processing activities of the Supplier and its subcontractors according to accepted audit plan upon twelve (12) working days' prior written notice. If any audit reveals that the Services are in non-compliance with this Appendix, Agreement or the Laws, Supplier shall take all necessary measures at its sole expense to ensure that the Services become compliant with the applicable provisions. Purchaser shall be entitled to verify the compliance by another audit at any time after the implementation of such corrective measures.

Purchaser is responsible for the costs of the audits. However, should the audit reveal any material violation or breach of this Appendix by Supplier, Supplier shall without delay compensate Purchaser for the costs arising from the remedy of the breach.

The Supplier shall comply with any decisions from the Data Protection Authority (Sw. *Datainspektionen*) or other competent authority in respect of the Personal Data which is processed on behalf of the Purchaser. The Supplier shall also allow any competent authority to conduct supervision of the processing which takes place.

6. HANDLING OF DATA BREACHES

In the event of a Personal Data Breach, or any other threatening enforcement proceeding against the Supplier pertaining to the processing of Personal Data, the Supplier will provide Purchaser with an accurate written notice immediately upon becoming aware of it, and in no event later than within forty-eight (48) hours. Supplier shall work with Purchaser's prior approval on quickly resolving the issue, and prevent further losses, and provide any notices to an individual or government authority containing the information as mandated by the Laws. Supplier will also, upon Purchaser's prior request, provide any appropriate remedial services to individuals.

7. RIGHTS OF THE DATA SUBJECTS

If requested by Purchaser in order for Purchaser to comply with the Laws, Supplier shall at reasonable cost based on actual work by Supplier: (a) promptly provide Purchaser with a copy of individuals' Personal Data in tangible and/or machine readable form; (b) promptly correct, block or delete individuals' Personal Data; (c) promptly provide Purchaser with such information and cooperation regarding the processing of Personal Data under the Agreement as Purchaser may reasonably request; and (d) provide individuals whose Personal Data is being processed with such information regarding the processing as Purchaser may reasonably request.

In the event a public authority or a third party requests such information as follows from the section above, the Supplier shall immediately notify the Purchaser of the request and the Supplier and Purchaser shall, in consultation, agree on the appropriate manner of proceeding.

Semantix

8. **INDEMNIFICATION**

Supplier shall defend, indemnify and hold Purchaser harmless from and against any claims, actions, damages, losses, costs and expenses, including but not limited to reasonable attorneys' fees, arising out of or resulting from any Third Party claim against Purchaser or its affiliates arising out of or resulting from Supplier's failure to comply with any of its obligations under this Appendix.

In the event of any claim by a Third Party against Supplier concerning the infringement of Laws that concern Personal Data relating to Purchaser employees (current and former), job applicants, external workforce or customers (prospective, current and former), Supplier shall reserve Purchaser the right either independently or as an intervener to participate in any discussions, negotiations or legal proceedings, at Supplier's expense, in order to ensure the protection of its rights. If the Third Party's claim turns out to be frivolous, Supplier shall not be obliged to compensate Purchaser for any costs incurred by Purchaser. In any other case Supplier shall be liable for any and all costs, expenses, compensations, losses and damages caused to Purchaser due to such Third Party claims.

No limitation of liability shall be applicable to damage or losses arising out of a breach of this Appendix.

9. **TERMINATION**

This Appendix shall remain in full force for as long as the Agreement is in force and for such period thereafter as is necessary for the activities after Agreement termination or expiration to be completed. To the extent that Personal Data is processed by or for Supplier, for whatsoever reason, after the termination or expiration of the Agreement, this Appendix shall continue to apply to such Processing for as long as such processing is carried out.

Breach by Supplier (or its subcontractors, as the case may be) of its obligations under this Appendix will be deemed a material breach of the Agreement.

Obligations which by their nature should survive termination or expiration of the Agreement, shall so survive.

In case of any conflict between the terms of this Appendix and the Agreement, the provisions of this Appendix shall prevail. Any changes to this Appendix must be agreed in writing between the Parties.

Semantix

Annex 1: Instructions for Processing Personal Data

This Annex includes details of the Processing of Personal Data as required by Article 28(3) in the GDPR.

Subject-matter of the processing	The subject-matter of the processing is language and DTP services as well as machine translation engine training as defined in the Service Agreement (Framework Agreement or Order Confirmation) concluded between Purchaser and Supplier.
Duration of the processing	For as long as the Service Agreement between Purchaser and Supplier is in force, unless otherwise agreed upon, and as long as needed according to applicable Laws.
Nature and purpose of the processing	Supplier will provide language-related services such as but not limited to, translation, revision, review, editing, copywriting, interpreting, language training, DTP and/or machine translation engine training, as ordered by the Purchaser. Supplier may process documents using CAT tools that store the content of the documents (including Personal Data) in a translation memory specific to Purchaser. Furthermore, such data is used to create and train custom machine translation engines.
Type of Personal Data Purchaser may submit Personal Data to Supplier, the extent of which is determined and controlled by Purchaser.	First and last name Job title/position Employer Contact information (company, email address, phone number, address) ID data Professional life data Personal life data Connection data Localisation data Bank account data Purchase history Additionally, other Personal Data that the Supplier receives in the context of the Agreement.
Special categories of data Purchaser may submit special categories of data to Supplier, the extent of which is determined and controlled by Purchaser.	Personal data revealing racial or ethnic origin Personal data revealing political opinions Personal data revealing religious or philosophical beliefs Personal data revealing trade union membership Genetic data

Semantix

	Biometric data for the purpose of uniquely identifying a natural person Data concerning health Data concerning a natural person's sex life or sexual orientation
Categories of Data Subjects Purchaser may submit Personal Data relating to the following categories of Data Subjects to Supplier, the extent of which is determined and controlled by Purchaser.	Employees of Purchaser Customers of Purchaser Suppliers of Purchaser Freelancers of Purchaser Business partners of Purchaser Natural persons mentioned in documents sent to Supplier by Purchaser for processing. Additionally, other Data Subjects that are included in the context of the Agreement.
Countries/locations data will be exported to The Personal Data will be processed (remotely accessed or hosted) in the following countries/locations:	Primarily EU/EEA countries, however, Supplier works with a global network of freelancers and agencies within language, DTP and machine translation services. Personal Data may therefore also be processed outside EU/EEA. All subcontractors handling Personal Data must sign a Data Processing Agreement that complies with the GDPR and agree to the Model Clauses or provide a similar suitable safeguard.

Semantix

Annex 2: Subcontractors

Approved categories of subcontractors engaged in processing Personal Data

The Supplier is entitled to use the following approved categories of subcontractors:

Translators;
Revisers;
Reviewers;
Editors;
Copywriters;
DTP suppliers;
Interpreters; and
Language Trainers

that form part of Supplier's global network and are used for specific linguistic tasks, to the extent their services are necessary for handling the matter at hand.

Purchaser may at any time request a list of the specific subcontractors carrying out the processing activities in relation to one or more specific tasks.

Approved subcontractors engaged in processing Personal Data in systems

The Supplier is entitled to use the following subcontractors for processing Personal Data in systems:

Subcontractor	Address	Organisation number
Memsource a.s.	Spalena 51 110 00 Prague 1 Czech Republic	CZ 24707139
WebProof A/S	Rådhuspladsen 16 1550 Copenhagen Denmark	DK 25452976
iLangL	Tussen de Bogen 52 1013 JB Amsterdam, Netherlands	NL8552.95.399.B.01
One2Edit	1io Germany Mozartstraße 5 87435 Kempten Germany	DE815616575
Microsoft Translator	Redmond WA 98052-7329 USA	IE8256796U

Annex 3: Model Clauses