

Data Processing Appendix, Suppliers, Language Solutions (Appendix 3)

This Data Processing Appendix ("**Appendix**") is between:

("Supplier" / "Subprocessor")

and

Semantix ("**Purchaser**" / "**Processor**"), i.e., the companies listed in the Supplier Agreement, or any other company being part of the Semantix group of companies ("Semantix") from time to time as defined in the Purchase order.

Supplier and Purchaser acknowledge that from time to time, Purchaser may request Supplier to perform Services with respect to the Personal Data. Such Personal Data is subject to Data Protection Laws that require Supplier and Purchaser each to treat Personal Data securely, confidentially and in accordance with all Data Protection Laws.

Accordingly, in consideration of the mutual obligations set out herein, Supplier and Purchaser hereby agree as follows.

1. Definitions

In this Appendix, the following terms shall have the meanings set out below:

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

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

"**Data Subject**" shall mean an identified or identifiable natural person; i.e. 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 General Data Protection Regulation 2016/679 and any amendments, replacements or renewals thereof, as well as all other applicable binding data protection, privacy or data security directives, laws, regulations and rulings when processing Personal Data under the Agreement.

"**Third Countries**" means any country outside the EEA or outside any other country with Data Protection Laws restricting transfers of Personal Data to certain countries.

"**Standard Contractual Clauses**" shall mean the standard contractual clauses annexed to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of

Data Processing Appendix, Suppliers, Language Solutions (Appendix 3)

Personal Data to third countries pursuant to Regulation (EU) 2016/679 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 sub-processors 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 services and other activities to be supplied to or carried out by or on behalf of Supplier for Purchaser pursuant to the Supplier Agreement;

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

“EEA” means the European Economic Area.

“GDPR” means EU General Data Protection Regulation 2016/679.

“Supplier Agreement” means, that certain Supplier Agreement executed by Purchaser (or a subsidiary thereof) and Supplier, together with any subsequent purchase order, work order or statement of work entered into in connection with Services to be performed by Supplier for the benefit of Purchaser or an affiliate or subsidiary thereof.

“Restricted Transfer” means:

- an onward transfer of Personal Data from the Supplier to a subprocessor, or between two establishments of the Supplier; or
- in each case, where such transfer would be prohibited by Data Protection Laws in the absence of the protection for the transferred Personal Data afforded pursuant to this Addendum.

2. Processing of personal data

The Parties acknowledge that for purposes of this Appendix, Purchaser is Processor and Supplier is Subprocessor of Personal Data. This Appendix sets forth the requirements applicable to Personal Data processed by Supplier or through Supplier’s systems in connection with providing the Services.

Annex 1 hereto sets out the Parties’ understanding of the Personal Data to be processed by Supplier pursuant to this Appendix, as required by Articles 28(3) and 28(4) of the GDPR. Purchaser will inform Supplier of any changes to any such Annex required to reflect Purchaser’s actual use of the Services. Supplier shall not Process Personal Data other than on Purchaser’s instructions on behalf of Controller, unless Processing is required by applicable

Data Processing Appendix, Suppliers, Language Solutions (Appendix 3)

laws to which the Supplier is subject, in which case Supplier shall to the extent permitted by law inform Purchaser of that legal requirement before the relevant Processing of Personal Data.

Supplier shall:

- comply with all applicable Data Protection Laws in the Processing of Personal Data; and
- comply with written instructions of Purchaser or data protection authorities provided to supplier, e.g., on handling, protecting, and encrypting Personal Data; and
- 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 Purchaser is to take place, the Supplier shall ensure that any such instruction or information is obtained from Purchaser.

Annex 1 to this Appendix sets out certain information regarding the processing of Personal Data as required by Articles 28(3) and 28(4) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Purchaser may make reasonable amendments to Annex 1 by written notice to Supplier from time to time as Purchaser reasonably considers necessary.

3. Subprocessing

Supplier is prohibited from appointing, engaging, or retaining additional subprocessors to Process Personal Data provided by Purchaser.

4. Deletion or return of Personal Data

Supplier shall, within 90 days after delivery of any Services involving the Processing of Personal Data, securely delete all copies of Personal Data received from Purchaser.

Supplier shall ensure the confidentiality of all Personal Data and shall ensure that such Personal Data is only processed as necessary for the purpose(s) specified in the Applicable Laws.

5. Data disclosures

Supplier shall immediately notify Purchaser about any requests from governmental authorities regarding access to Purchaser's Personal Data, unless such notification is prohibited by applicable law. Supplier should not respond to such a request without Purchaser's prior written approval.

6. Transfer of Personal Data

Supplier must not transfer or process Personal Data to a Third Country without written approval from Purchaser. If Purchaser approves of such transfer, Supplier shall take all measures (including but not limited to SCC) necessary to make sure the transfer is performed in accordance with all applicable Data Protection Laws, including at least EU's Data Protection Laws.

Data Processing Appendix, Suppliers, Language Solutions (Appendix 3)

If Purchaser approves a transfer to Supplier, Purchaser and each Purchaser Affiliate (each as “data exporter”) and Supplier (“data importer”), hereby enter into the Module 3 SCC in respect of that transfer from Purchaser or any Purchaser Affiliate to Supplier governed by GDPR

Supplier may not perform any Restricted Transfer.

7. Security

Semantix (Purchaser) promises all its customers a minimum level of security. To comply with Laws, Purchaser must demand at least the same level of security of Supplier. Supplier shall, at all times, implement and maintain appropriate organisational, and technical measures to protect the Personal Data, so that all processing complies with the Laws and Purchaser’s written instructions. The security requirements are further described in Annex 1.

8. Audit rights

Purchaser may request a review of Supplier’s security documentation and/or a written report of self-assessment from Supplier. This is the most common form of auditing.

Purchaser (or an independent Third Party on its behalf) may audit the processing activities of Supplier and its sub-processors 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, Supplier 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.

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

9. Personal Data Breach

In the event of a Personal Data Breach, or any other threatening enforcement proceeding against Supplier related to the processing of Personal Data, Supplier will immediately upon becoming aware provide Purchaser with an accurate written notice, and in no event later than within twenty-four (24) hours.

- Supplier shall, with Purchaser’s prior approval, work on quickly resolving the issue, and prevent further losses.
- Supplier shall also provide any notices to an individual or government authority containing the information in accordance with the Law.
- Supplier will also, upon Purchaser’s prior request, provide any appropriate support to individuals.

10. Data Subject Rights

If requested by Purchaser in order for Purchaser to comply with the Laws, Supplier shall – at reasonable cost – based on actual work by Supplier:

- promptly provide Purchaser with a copy of individuals' Personal Data in a clear readable form;
- promptly correct, block or delete individuals' Personal Data;
- promptly provide Purchaser with such information regarding the processing of Personal Data under the Appendix as Purchaser may reasonably request; and
- 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 information as follows from the section above, Supplier shall immediately notify Purchaser of the request and Supplier and Purchaser shall, in consultation, agree on the appropriate manner of proceeding.

11. Indemnification

The Parties shall bear responsibility in accordance with Applicable Data Privacy Laws.

12. General Terms and Conditions

This Appendix shall remain in full force for as long as the Supplier 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 Supplier Agreement, this Appendix shall continue to apply to such Processing for as long as such processing is carried out.

Breach by Supplier of its obligations under this Appendix will be deemed a material breach of the Supplier Agreement.

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

13. Other

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

Any amendment, waiver or modification of this Appendix shall only be enforceable if in writing. Should any provision of this Appendix be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

This Agreement comes into force upon signature by the parties. In the event of any conflict or inconsistency between the terms of this Agreement and the terms of the Standard Contractual Clauses, the latter shall prevail.

Data Processing Appendix, Suppliers, Language Solutions (Appendix 3)

This document will be signed digitally. The person signing this Appendix on behalf of Supplier warrants that they have the right and authority to enter into this Appendix and bind Supplier to the obligations set forth herein.

Annex 1: Description of processing and security measures

This Annex includes certain details of the Processing of Personal Data as required by Articles 28(3) and 28(4) GDPR.

Subject matter and duration of the Processing of the Personal Data

The subject matter activities relevant to the data transferred under these Clauses shall be as set forth in the Supplier Agreement and in any related purchase order and shall depend on which of the services are selected by Purchaser.

The duration of the processing is set out in the purchase order addressing the scope of services.

The nature and purpose of the Processing of the Personal Data

The nature and purpose of the processing is to provide the services set forth in the Supplier Agreement and any related purchase order, as summarized above. Supplier will translate Personal Data contained within documents that Purchaser's customers retain Purchaser to translate, including, but not limited to, human resources documents, legal documents, medical documents, and business and operational documents.

The categories of Data Subject to whom the Personal Data relates

The categories of Data Subject to whom the Personal Data relates include, but are not limited to, Purchaser's customers' (and other third parties'), employees, contractors, clients (and their employees, clients, patients or end users) and study participants.

The types of Personal Data to be processed

The types of Personal Data to be Processed include, but are not limited to, names, addresses, contact information, date of birth, marital status, number of dependents, nationality, health status and data, biometric data, sexual orientation, religious or political beliefs, race, gender, ethnic background, genetic data, human resources data, hobbies, professions, user behavior data, log data and log files, survey data, video and photographic information, insurance data, payment information, account numbers and/or other personally identifiable information.

Special categories of Personal Data (if appropriate)

The Personal Data transferred concern the following special categories of Personal Data (please specify): the potential categories of data transferred is unlimited and may include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The obligations and rights of subprocessor

The obligations and rights of subprocessor, acting on behalf of processor, are set out in the Agreement.

Technical and organisational measures

Technical safeguards shall include all technical security controls defined by Supplier, following the recommendations as laid out in ISO/IEC 27000 series (or equivalent) 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

Data Processing Appendix, Suppliers, Language Solutions (Appendix 3)

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.

Supplier warrants that in performing the Services under the Appendix 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.