languagewire

DATA PROCESSING AGREEMENT

Schedule 3

1. PREAMBLE

1.1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

1.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

1.3. In the context of the provision of services as specified in an agreement between the parties, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

1.4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

1.5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

1.6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject, and duration of the processing.

1.7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.

1.8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor, and how audits of the data processor and any sub-processors are to be performed.

1.9. Appendix D contains provisions for other activities which are not covered by the Clauses.

1.10. The Clauses, along with appendices, shall be retained in writing, including electronically, by both parties.

1.11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject, pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

2.1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions, and the Clauses.

2.2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

2.3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

3.1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

3.2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

3.3. If the data controller gives an unlawful instruction, the data processor can decline to follow the unlawful instructions. If the data processor follows the unlawful instruction, the data controller is responsible for consequential damages including claims cf. D.2.

4. CONFIDENTIALITY

4.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality, or are under an appropriate statutory obligation of confidentiality, and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

4.2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5. SECURITY OF PROCESSING

5.1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymization and encryption of personal data;

b. The ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

5.2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

5.3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organizational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6. USE OF SUB-PROCESSORS

6.1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

6.2. The data processor shall therefore not engage another processor (sub-processor) for the fulfillment of the Clauses without the prior general written authorization of the data controller.

6.3. The data processor has the data controller's general authorization for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorized by the data controller can be found in Appendix B.

6.4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

6.5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business-related issues that do not affect the legal data protection content of the sub-processor agreement shall not require submission to the data controller.

6.6. If the sub-processor does not fulfill his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfillment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

7.1. Any transfer of personal data to third countries or international organizations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

7.2. In case transfers to third countries or international organizations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

7.3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

a. Transfer personal data to a data controller or a data processor in a third country or in an international organization;

b. Transfer the processing of personal data to a sub-processor in a third country

c. Have the personal data processed in by the data processor in a third country

7.4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

7.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8. ASSISTANCE TO THE DATA CONTROLLER

8.1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfillment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. The right to be informed when collecting personal data from the data subject;

b. The right to be informed when personal data have not been obtained from the data subject;

c. The right of access by the data subject;

d. The right to rectification;

e. The right to erasure ('the right to be forgotten');

f. The right to restriction of processing;

g. Notification obligation regarding rectification or erasure of personal data or restriction of processing;

h. The right to data portability;

i. The right to object; and

j. The right not to be subject to a decision based solely on automated processing, including profiling.

8.2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 5.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, at the place of the data controller's domicile, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. The data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. The data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment)

d. The data controller's obligation to consult the competent supervisory authority, at the place of the data controller's domicile, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

8.3. The parties shall define in Appendix C the appropriate technical and organizational measures by which the data processor is required to assist the data controller, as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clauses 8.1. and 8.2.

9. NOTIFICATION OF PERSONAL DATA BREACH

9.1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

9.2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

9.3. In accordance with Clause 8(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. The likely consequences of the personal data breach;

c. The measures taken or proposed to be taken by the controller to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

9.4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10. ERASURE AND RETURN OF DATA

10.1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so, unless Union or Member State law requires storage of the personal data.

11. AUDIT AND INSPECTION

11.1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

11.2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

11.3. The data processor shall be required to provide the supervisory authorities who, pursuant to applicable legislation, have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities upon presentation of appropriate identification.

12. THE PARTIES' AGREEMENT ON OTHER TERMS

12.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying, e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13. COMMENCEMENT AND TERMINATION

13.1. The Clauses shall become effective on the date of both parties' signature.

13.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

13.3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

13.4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 10.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

13.5. Signature

These Clauses shall be considered as an integrated part of the agreement between the parties and is attached to the agreement as an appendix/schedule.

These Clauses shall therefore be considered as entered when entering into the agreement.

14. DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS

14.1. The parties may contact each other using the following contacts/contact points:

The data controller's contact/contact point is specified in the agreement between the parties.

The data processor's contact/contact points are the following:

Name	Sebastian Kraska
Position	Data Protection Officer
Telephone	+49 89 1891 7360
E-mail	data_protection@languagewire.com

14.2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Appendix A: Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To deliver the services as requested by the data controller in accordance with the agreement between the parties; in particular, to provide translation services to the controller.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Storage, adaptation, or alteration in connection with services delivered by the data processor including, for example, translation, analyzing, support, etc. as specified in the agreement between the parties.

A.3. The processing includes the following types of personal data about data subjects:

The data processor shall process the types of personal data that the data controller directly or indirectly gives the data processor access to, which typically includes:

- Ordinary categories of personal data cf. article 6 of the General Data Protection Regulation, incl. the following types of personal data: Name, Address, Age, E-mail, Phone number, Pictures.

A.4. Processing includes the following categories of data subject:

The data processor shall process personal data about the categories of data subjects that the data controller directly or indirectly gives the data processor access to, which typically includes:

- Employees, B2B Customers, B2C Customers and vendors

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

These Clauses shall be effective for the duration of the provision of the services in accordance with the agreement and shall terminate automatically when the data processor no longer processes personal data on behalf of the data controller as part of the services.

Appendix B: Authorized Sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorizes the engagement of the following sub-processors:

Sub-processors for general services:

Entity:	Reg. no.:	Address:	Description of data processing:	Transfer of personal data outside the EU/EEA:
Google Cloud Platform (GCP)	HRB 86891	ABC-Strasse 19, Hamburg, Germany, 20354	Hosting of cloud platform infrastructure services	No.
Microsoft Azure	IE 8256796 U	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Hosting of cloud platform infrastructure services	No.
Sentia Denmark A/S	CVR: 10008123	Copenhagen Region, Lyskaer 3A, 2730, Herlev, Denmark	Private cloud, self-hosted Infrastructure	No.
Zendesk	CVR: 30801830	989 Market Street, San Francisco, CA 94103, USA	Customer Support Services	No.
Blackbird International, Inc.	EIN: 92-3568729	Blackbird International Inc., 16192 Coastal Highway Lewes, Delaware 19958, USA	Connector for transfer of data from Customer to LanguageWire Platform.	No.

Compliance information:
The data processor hosts services with Google Cloud Platform, MS Azure, & Sentia.

- Google Cloud Platform is SOC 1, SOC 2, SOC 3 and ISO 27001 certified. More details about Google Cloud Platform's compliance can be found on https://cloud.google.com/security/compliance
- Microsoft Azure is SOC 1, SOC 2, SOC 3 and ISO 27001 certified. Specific details about Microsoft Azure's compliance programs can be found on https://docs.microsoft.com/en-us/azure/compliance.
- Sentia is ISAE 3402 certified.

Google Cloud Platform, Microsoft Azure, and Sentia have designed their data center infrastructures to provide optimum availability while ensuring complete customer privacy and segregation.

Risk assessment has been conducted for the list of authorized sub-processors above.

General authorization of sub-processors for translation and language services:

The data controller accepts that an order for translation or language services containing personal data shall constitute an authorization for the addition of sub-processors for a limited duration as necessary for the provision of the agreed services. The addition and replacement of sub-processors for translation and language services shall not be subject to the notice periods described below in Appendix B.2.

The data controller may at any time request a list of the sub-processors previously or currently used for the provision of translation or language services by providing the data processor with a written notice containing the information necessary to identify the relevant order(s).

B.2. Prior notice for the authorization of sub-processors

The data processor's notice of any planned changes in terms of addition or replacement of sub-processors must be received by the data controller no later than thirty (30) days before the addition or replacement is to take effect, in so far as this is possible.

Regardless of the above, the data controller accepts that there may be situations with a specific need for such change in terms of addition or replacement of sub-processors with a shorter notice, or immediately.

If the data controller has any objections to such changes, the data controller shall notify the data processor thereof without undue delay before such change is to take effect. The data controller may only object to such changes if the data controller has reasonable and specific grounds for such refusal.

In case of the data controller's objection, the data processor may be prevented from providing all or parts of the agreed services. Such non-performance cannot be ascribed to the data processor's breach. The data processor will maintain its claim for payment for such services regardless even if they cannot be provided to the data controller unless the controller's objection was based upon reasonable and specific grounds.

Appendix C: Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Storage, adaptation, or alteration in connection with services delivered by the data processor including, for example, translation, analyzing, support, etc. as specified in the agreement between the parties.

C.2. Security of processing

The level of security shall take into account:

The data processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with the processing activities that the data processor performs for the data controller.

The technical and organizational measures are determined by taking into account the current technical level, the implementation costs, the nature, scope, coherence, and purpose of the treatment in question, as well as the risks of varying probability and seriousness for the rights and freedoms of natural persons.

In assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular, in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored, or otherwise processed.

The data processor is then entitled and obliged to make decisions about which technical and organizational security measures must be implemented in order to establish the necessary (and agreed) level of security.

The data processor shall, however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

The data processor ensures that the data is encrypted in transit throughout the entire flow by means of HTTPS, SSL, TLS, and Encryption at rest (AES-256) for backend services. Pseudonymization is applied to Meta data, used for analytical and performance monitoring. No personal data is stored after the transaction has expired.

- The data processor designs the products to be highly available, fault-tolerant, and fault- resilient. To achieve this, the data processor follows the industry's best practices which the data processor continuously improves on and reviews.

The data processors use active-active / active-passive modes, and actively load balance data and services between availability zones within the data processor's Cloud Service Providers platform (Google Cloud Platform & Microsoft Azure) to minimize the potential impact and recovery time of the data processor's services.

The data processor runs an agile software development lifecycle (SDLC) process.

The data processor passes all software changes through a formalized code review process, which is approved by the relevant Team Lead prior to being released into isolated environments. Upon successful testing and quality assurance, the changes are promoted into production. All of the data processor's development is in-house.

All of the data processor's backend infrastructure ships logs to a centralized solution where they are aggregated, reviewed, and analyzed. The data processor does not store logs locally.

The data processor's engineering team and team members are only granted access to the data processor's logs based on their work-related needs. Examples of logged activities are:

- Application exceptions
- Stack trace
- Performance statistics
- Backend changes and deployments
- Malicious activity and exceptions

The data processor's logs are confidential and not made available outside. The logs are stored in a secure, tamperproof manner and cannot be manipulated or changed.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clauses 8.1. and 8.2. by implementing the following technical and organizational measures:

At the specific request of the data controller, the data processor, taking into account the nature of the processing, assists the data controller as far as possible by appropriate technical and organizational measures in compliance with the data controller's obligation to respond to requests for data subjects' rights.

If a data subject submits a request for the exercise of his rights to the data processor, the data processor shall notify the data controller without undue delay.

Taking into account the nature of the processing and the information available to the data processor, the data processor, upon specific request, assists the data controller in ensuring compliance with the data controller's obligations in relation to:

- Implementation of appropriate technical and organizational measures
- Security breaches
- Notification of breach of personal data security to the data subject
- Conducting impact assessments
- Prior consultations with a supervisory authority

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 10.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses. Personal data stored throughout the term of the agreement shall be stored in accordance with the data processor's standard data retention policy or, as specifically agreed upon with the data controller, from time to time.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Primarily from the data processor or the sub-processors' locations, including locations under their and their employees' control.

C.6. Instruction on the transfer of personal data to third countries

The data processor is only allowed to transfer personal data to a country outside the European Union or EEA (a "Third Country") or an international organization located in a Third Country as further specified below.

6.1 General approval of transfer of personal data to secure Third Countries

With the Clauses, the data controller provides a general and prior approval (instruction) for the data processor to transfer personal data to Third Countries if the European Commission has determined that the Third Country/the relevant area/the relevant sector has a sufficient level of protection.

6.2 Approval of transfer to specific recipients of personal data in Third Countries subject to appropriate safeguards

The data controller instructs the data processor to transfer personal data to Third Countries when necessary in order for the data processor to deliver the service in accordance with the agreement, including by using the listed sub-processors transferring personal data to Third Countries as stated in Appendix B. Furthermore, the data processor shall be entitled to transfer personal data to Third Countries if the data controller's acts result in such a transfer.

The data processor is only allowed to transfer data to a Third Country if the data processor, prior to the transfer, has secured the adequate safeguards to ensure compliance with applicable Danish data protection laws, including the General Data Protection Regulation.

This entails that the data processor must ensure that:

- An approved transfer tool is in place;
- An assessment of the impact of the transfer, based on the laws and practices in the third country as well as the safeguards in place, (a "transfer impact assessment") is carried out and documented; and

In case the European Commission completes new Standard Contractual Clauses subsequent to the formation of the original Standard Contractual Clauses, the data processor is authorized to renew, update, and/or use the Standard Contractual Clauses in force from time to time.

The content of these Clauses shall not be deemed to change the content of such safeguards, including the European Commission's Standard Contractual Clauses. If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

Pursuant to Articles 24 and 28 of the General Data Protection Regulation, the data controller is entitled and obliged to monitor the data processor's processing of personal data on behalf of the data controller. The data controller's monitoring of the data processor may consist in one of the following actions from the data controller:

- Self-checking based on documents provided to the data controller by the data processor;
- Written inspection; or
- Physical inspection.

7.1 Self-checks

The data controller may ask questions regarding supervision to the data processor and the data controller can, at his or her request, access a range of documents for the purpose of self-checking, including:

- A description of the physical and organizational security measures at the data processor;
- Risk assessment – of shared infrastructure (firewall, backup, etc.);
- IT security policy; and
- The data processor's contingency plans.

7.2 Written inspection and physical inspection

The data controller may choose to carry out an inspection either as a written inspection or as a physical inspection. The inspection may be carried out by the data controller and/or in cooperation with a third party. An inspection must be based on the security measures agreed between the parties.

Procedure and reporting of written inspection or physical inspection:

- The data controller shall contact the data processor by e-mail to data_protection@languagewire.com with request for a written and/or physical inspection.
- At written inspections the data controller shall give notice to the data processor hereof without undue delay.
- At physical inspections the data controller shall arrange a date for the inspection in advance with the data processor.
- The data processor confirms receipt and confirms the date for such inspection.
- The inspection is made.
- The data controller drafts a report that is subsequently sent to the data processor.
- The data processor will review the draft report and provide potential comments to the data controller's observations (can be repeated several times).
- The final report is concluded by the data controller.
- The inspection is ended.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor regularly audits its sub-processors using a risk-based approach based on the best practices for such audits generally applied from time to time. Such audits may include review of audit reports, use of questionnaires, and other appropriate means.

If the competent supervisory authority makes an inspection, e.g. because of a data breach, the costs related to the inspection and the time rests with the controller.

Appendix D: The parties' terms of agreement on other subjects

D.1. In general

In relation to the data processor's processing of personal data on behalf of the data controller, the parties have agreed on the specific terms outlined below.

In case of discrepancy between the Clauses and the terms laid down in this appendix D, appendix D shall take precedence.

D.2. Consequences of the data controller's unlawful instructions

The data controller is aware that the data processor depends on the data controller's instructions to which extent the data processor is entitled to use and process personal data on behalf of the data controller.

If the data controller's instruction is considered unlawful according to the data processor's reasonable evaluation, the data processor is able to end further processing than storage until the data controller gives supplementary instruction on whether the processed personal data once again can be processed legally or if the personal data shall be handed over or deleted. The data processor's end of processing in such situations cannot lead to breach of these Clauses or the agreement between the Parties.

The data processor is not liable for any claims arising from the data processor's acts or omissions, to the extent such acts or omissions are a direct data processing activity exercised in accordance with the data controller's instructions, and if the data processor is held liable or sanctioned, the data controller shall hold the data processor harmless.

D.3. Implementation of other security measures

The data processor is entitled to implement and maintain other security measures than those specified in the Clauses and Appendix C.2; however, provided that such other security measures as a minimum provide the same level of security as the described security measures.

D.4. Use of sub-processors supplying on standard terms

The data processor shall be obliged to impose such clauses unto its sub-processors which ensure a minimum level of protection as set out in Article 28 of the GDPR, and to the extent reasonably possible, as necessary to ensure a level of protection equivalent to what is upon agreed with the data controller under the Clauses.

Regardless of Clause 6, it is emphasized that if the data processor uses a sub-processor, who provides services on its own terms, which the data processor cannot deviate from, the sub-processor's terms for such processing performed by such sub-processor will apply. If processing is subject to a sub-processor's terms, this will be specified in Appendix B, and such standard terms will be forwarded to the data controller at the data controller's request.

With these Clauses, the data controller accepts and instructs that such specific processing activities are based on the sub-processor's terms.

D.5. The data controller's objection to a sub-processor

If the data controller has any objections to the application of a sub-processor, the data controller shall notify the data processor thereof without undue delay before such change is to take effect as described in Appendix B.2. The data controller may only object to such changes if the data controller has reasonable and specific grounds for such objection.

In case of the data controller's objection, the data processor may be prevented from providing all or parts of the agreed services. Such nonperformance cannot be ascribed to the data processor's breach. The data processor will maintain its claim for payment for such services regardless, even if they cannot be provided to the data controller unless the data controller's objection was based on reasonable and specific grounds.

D.6. Compensation

The data processor is entitled to receive reasonable payment for time spent as well as other direct costs incurred by the data processor relating to assistance and services provided by the data processor to the data controller. Such assistance and services may include, but is not limited to, assistance and service described in Clauses 8, 9, 11, C.3 and C.7, changes to the instruction, cooperation with supervisory authorities, etc.

The compensation is calculated on the basis of the time spent and the agreed hourly rates regarding the data processor's provision of services to the data controller, and if no hourly rates have been agreed on, the data processor's current hourly rates will be applied, with the addition of any cost paid, including also cost to be paid by the data processor for the assistance of sub-processors.

The data processor shall not be entitled to compensation for time spent in relation to the handling of personal data breaches caused by the data processor nor for time spent in relation to the handling of requests from data subjects where the data processor's solutions and services does not technically enable the data controller to handle the request without assistance from the data processor.

Regardless of the above, a party does not have the right to claim compensation for assistance, service, or implementation of changes to the extent where such assistance or changes are a direct consequence of the party's own breach of these Clauses.

D.7. Limitation of liability

Any limitations of liability agreed between the data processor and the data controller applies to the data processor's processing of personal data under these Clauses, including claims related to article 82 of the General Data Protection Regulation.

languagewire

en-US
05/2024