Last updated: September 4, 2020

GDPR Addendum to the Services Agreement

Between **Customer**

hereinafter referred to as "**(Data) Controller**"

and

Amazon Europe Core S.à.r.l. ("AEC")

hereinafter referred to as "**(Data) Processor**"

each referred to as a "**Party**"
together referred to as the "**Parties**"

Preamble

1. This General Data Protection Regulation Addendum ("**GDPR Addendum**") is incorporated by reference into the Services Agreement (as defined below) and all related orders for Sizmek Services (defined below) between Customer (as defined below) and the applicable Sizmek entit(y/ies) named in the Services Agreement. This GDPR Addendum applies to the extent that the Data Protection Law applies to the processing of Personal Data pursuant to the Services Agreement.

2. This GDPR Addendum is supplemental to the Services Agreement and sets out the terms that apply when Personal Data (as defined below) is processed by AEC and/or its Affiliate designees under the Services Agreement. The purpose of the GDPR Addendum is to ensure such processing is conducted in accordance with applicable laws, including the Data Protection Law (defined below), and with due respect for the rights and freedoms of individuals whose personal data are processed.

3. Sizmek provides the Services and the Data Controller uses the Services for the purposes specified in the Services Agreement. With respect to the Services Agreement, the Data Processor processes Personal Data on behalf of, and as instructed by, the Data Controller.

4. This GDPR Addendum details the Parties' rights and obligations related to the scope of the processing of Personal Data. Subject to paragraph 1 above, this GDPR Addendum shall apply to all activity within the scope of and related to the Services Agreement, and in whose context the Data Processor's employees or subcontractors may come into contact with Data Controller's Personal Data.

5. This GDPR Addendum applies solely to Sizmek by Amazon Services, including Sizmek Ad Suite services, and not to other services provided by Amazon or its Affiliates, unless otherwise agreed by the parties in writing.

How this GDPR Addendum Applies

1. If a Customer entity is a party to the Services Agreement, the Customer entity that is a party to the Services Agreement is a party to this GDPR Addendum.

2. If a Customer entity has executed orders under the Services Agreement but is not a party to the Services Agreement, this GDPR Addendum will be incorporated in such order(s), with the Customer entity that has executed such orders as a party hereto.

3. If a Customer entity is lawfully permitting an Affiliate (defined below) to use the Services specified in a Services Agreement, that Customer Affiliate is a party to this GDPR Addendum.

4. If a Customer enters into this GDPR Addendum on behalf of a third-party controller, Customer represents and warrants to Data Processor that Customer's instructions in respect of the processing by Data Processor of Personal Data have been notified to, and authorized by, the third-party controller of Personal Data, in accordance with Customer's obligations under the Data Protection Law.

5. This GDPR Addendum will not be valid and legally binding if the applicable Customer entity is not a party to the Services Agreement or order(s), is not a Customer Affiliate lawfully permitted to use the Sizmek Services, or is an indirect customer through an authorized reseller of Sizmek. An indirect customer should contact the authorized reseller about its contract with that reseller.

Section 1
Definitions

Affiliate(s): has the same meaning ascribed to it in the Services Agreement and, if not defined in the Services Agreement, means any legal entity directly or indirectly controlling, controlled by or under common control with a Party.

Customer: means the non-Sizmek or non-AEC party to both the Services Agreement and this GDPR Addendum that uses the Services.

Data Protection Law: means (i) the GDPR and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, (ii) the applicable data protection laws of the United Kingdom; and (iii) the applicable data protection laws of the country in which AEC is located.

Data Subjects: means the individuals whose Personal Data is being processed hereunder.

Personal Data: means the personal data (as defined in Data Protection Law) about any natural person supplied or collected by or on behalf of Customer.

Services: means the System and other services of Sizmek that process Personal Data and that are used by Customer pursuant to a Services Agreement for the delivery of digital advertisements to digital advertising media, and data enablement, creative optimisation, media execution and reporting services to create effective digital advertising and marketing campaigns.

Services Agreement: means each currently effective agreement between Sizmek and Data Controller pursuant to which Data Processor processes Personal Data for Data Controller.

Sizmek: means the Sizmek entity that is a party to the Services Agreement, AEC or any of its applicable Affiliates.

Standard Contractual Clauses: means the standard contractual clauses promulgated pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, as set forth in **Schedule C**, attached to and forming part of this GDPR Addendum.

Section 2
Subject of GDPR Addendum (Data Processing)

1. The scope, extent, duration and nature of the collection, processing and use of Personal Data as well as the types of Personal Data and categories of Data Subjects are set out in the Services Agreement and/or **Schedule A** attached hereto and both the Data Controller and Data Processor shall comply with all applicable requirements of the Data Protection Law.

2. The Data Controller selected Sizmek as a service provider by exercising its duties of diligence under the Data Protection Law. It is the intent of the Parties that the Services Agreement includes a written mandate within the meaning of the Data Protection Law and governs the Parties' rights and obligations in the context of data processing.

3. To the extent this GDPR Addendum employs the term "(data) process(ing) (of data)," it refers, in a general way, to the collection, processing, and use of Personal Data, including but not limited to obtaining, storing, altering, transmitting, blocking, deleting, using, anonymising, pseudonymising, encrypting or otherwise using data within the meaning of the Data Protection Law.

4. Direction means the written instruction issued by the Data Controller to Sizmek or the Data Processor, and directing the latter to perform a specific action with regard to Personal Data (e.g. processing, anonymisation, blocking, deletion, disclosure). "Written direction" includes input by Data Controller into the Sizmek's computer systems using Data Controller's log-ins to the Services.

Section 3
Data Controller's Rights and Obligations

1. The Data Controller is responsible (within the meaning of the Data Protection Law) for the Data Processor's processing of data. Data Controller shall ensure it has all necessary appropriate consents and notices in place to enable lawful transfer of Personal Data to, and processing of Personal Data by, the Data Processor for the duration and purposes of the Services Agreement.

2. The Data Controller is entitled to issue supplementary directions at any time regarding the purpose, manner and extent of the processing. The Data Controller shall bear any additional costs arising from this; the Data Processor is entitled to demand an advance payment. The Data Processor may refuse performing additional or modified data processing, in which case (i) the Data Controller and Data Processor may agree to accordingly reduce the scope of Personal Data processing by the Data Processor on behalf of the Data Controller or (ii) the Data Controller may terminate the Services Agreement and the Personal Data processing pursuant thereto.

3. The Data Controller shall ensure that Data Subjects' rights are observed and should third parties take legal action against the Data Processor or its Affiliates on the grounds of data processing, the Data Controller will indemnify the Data Processor and its Affiliates in respect of any such claim.

4. Prior to the commencement of data processing and in regular intervals thereafter, the Data Controller shall assure itself that the Sizmek has implemented technical and organisational measures to protect the Personal Data.

5. The Data Controller will promptly notify the Data Processor if and when it detects errors or irregularities in connection with the Data Processor's processing of Personal Data.

Section 4
Data Processor's Rights and Obligations

1. Without prejudice to the generality of Section 2 hereof, the Data Processor shall, in relation to any Personal Data processed in connection with the performance of obligations under the Services Agreement:

a. process that Personal Data only on the written instructions of the Data Controller unless the Data Processor is otherwise required by the laws of, as applicable, any member of the European Union or the United Kingdom, or by the laws of the European Union applicable to the Data Processor ("**Applicable Laws**"). Where the Data Processor is relying on Applicable Laws as the basis for processing Personal Data, the Data Processor shall promptly notify the Data Controller of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Data Processor from so notifying the Data Controller;

b. ensure that it has in place the appropriate technical and organisational measures set out in **Schedule B**, which have been reviewed and approved by the Data Controller, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, protecting confidentiality, integrity, availability and resilience of its systems and Services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

c. ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and

d. at the Data Controller's cost, assist the Data Controller: (i) in responding to any request from a Data Subject; (ii) in responding to requests, investigations or audits by a Data Protection Law supervisory authority or regulator (a "**DPA**"); and (iii) in complying with any request by Data Controller with respect to ensuring compliance with Data Controller's obligations under the Data Protection Law with respect to security, breach notifications, impact assessments and consultations with DPAs in connection with processing of Personal Data hereunder, provided that Data Processor shall notify Data Controller without undue delay should it receive any such request or query from a Data Subject or DPA;

e. notify the Data Controller without undue delay on becoming aware of a Personal Data breach;

f. at the written direction of the Data Controller, delete or return Personal Data and copies thereof to the Data Controller within reasonable time of termination of the Services Agreement unless required by Data Protection Law or permitted by Services Agreement to store the Personal Data; and

g. maintain complete and accurate records and information to demonstrate its compliance with this Section 4.

2. Data Controller agrees that Data Processor may transfer Personal Data outside of the European Economic Area or the United Kingdom, as applicable, pursuant to the Standard Contractual Clauses or an alternative recognized compliance standard for the lawful transfer of Personal Data outside such territory.

3. Data Processor has appointed a Data Protection Officer (DPO). The appointed person may be reached by contacting sizmek-legal@amazon.com.

Section 5
Subcontractors

The Data Controller consents to the Data Processor using third-party processors of Personal Data under this GDPR Addendum. The Data Processor confirms that it has entered or (as the case may be) will enter with the third-party processors into a written agreement incorporating terms which are substantially similar to those set out in this GDPR Addendum. As between the Data Controller and the Data Processor, the Data Processor shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this Section 5.

Section 6
Audit Rights

1. The Data Processor is obliged to assure compliance with the technical and organisational measures as set out in **Schedule B** by way of presenting upon request by Data Controller, a suitable opinion, or a report or excerpt of a report by an independent institution (e.g., accounting auditor, controller, internal or external data protection officer, IT security department, privacy auditor, quality auditor), or a suitable certification by an IT security or privacy audit ("**Report**"). The Report shall enable the Data Controller to reasonably assure itself of the Data Processor's compliance with the technical and organisational measures set out in **Schedule B**.

2. The Data Processor may refuse, at its own discretion and taking into account the Data Controller's statutory duties, to disclose certain information that is sensitive with respect to the Data Processor's business or if the Data Processor could violate statutory or contractual obligations by disclosing the information. In particular, the Data Controller is not granted access to information on the Data Processor's other business partners, on costs, on quality audit and contract management reports, as well as on any and all other non-public information of the Data Processor not directly necessary in view of statutory audit rights.

Section 7
Standard Contractual Clauses

The Standard Contractual Clauses will apply to Personal Data that is transferred outside the European Economic Area or the United Kingdom (as applicable), either directly or via onward transfer, to any country not lawfully recognised as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside such territory. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply if Data Processor has adopted an alternative recognised compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the applicable territory.

Section 8
Term of Addendum

Except where this GDPR Addendum expressly stipulates any surviving obligation, the term of this GDPR Addendum shall terminate upon termination or expiration of the Services Agreement.

Section 9
Miscellaneous

1. This GDPR Addendum shall constitute a binding part of the Services Agreement. Unless the foregoing has been regulated otherwise, the terms of the Services Agreement shall apply to this GDPR Addendum accordingly.

2. In the event that individual provisions of this GDPR Addendum are ineffective, the remaining provisions of the GDPR Addendum and the Services Agreement hereof continue in full force and effect. ‘

SCHEDULE A

DATA PROCESSING ACTIVITIES

In the provision of the Services as instructed by the Data Controller, Sizmek employs data collection technologies (such as advertising tags, pixels and cross-device graphs) on digital properties (such as digital advertisements, internet or mobile websites and mobile applications) that are designed to enable the collection and processing of pseudonymous data that may be Personal Data, including user agent identifiers (such as unique IDs associated with cookies and mobile advertising IDs), IP addresses, geographic data (latitude and longitude), and other non-personal metadata that is associated with such pseudonymous data (such as HTTP header data).

Depending upon the Services selected by the Data Controller and the instructions of the Data Controller regarding processing activities carried out by the Services, (including instructions received by the configuration of the Services by or at the direction of the Data Controller), Data Processor processes Personal Data to provide the Services, such as to serve digital advertisements into such inventory, to target digital advertisements to data subjects that comprise audiences created from the use of pseudonymous Personal Data about such data subjects, and to measure and report on data subjects' interactions with digital advertisements provided via the Services.

SCHEDULE B

TECHNICAL AND ORGANISATIONAL MEASURES

The Data Processor shall implement appropriate technical and organisational security measures to protect the Personal Data it processes from unintended or unauthorized access or disclosure, including but not limited to the following measures:

Physical security: When equipment and mobile units are not used, the equipment and the units are secured from unauthorized physical access or use and all access and use is under the direct physical supervision of an authorized individual.

Back-up copies: The Personal Data is backed up routinely. The copies are stored separately and with due care, ensuring that the Personal Data can be restored.

Control of access: Access to the Personal Data is limited by logical access controls. User-ID and password are not transferred. Procedures for the granting and closing of access are established by policy and controlled by an authorized administrator.

Communication of data: Excluding ad-serving data such as HTTP header data, which Data Controller acknowledges is transferred in an unsecure manner over the open internet, communication of the Personal Data should only take place in a secure environment.

Destruction of data: When equipment or mobile units containing Personal Data are no longer used to process Personal Data, the Personal Data is permanently deleted on the equipment, ensuring that the data cannot be restored.

SCHEDULE C

STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data Controller (as defined in the GDPR Addendum)

(the “data **exporter**”)

and

Sizmek (as defined in the GDPR Addendum)

(the “data **importer**”)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means 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.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect 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, and that 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;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(d) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity identified as “Data Controller” in the GDPR Addendum.

Data importer

The data importer is the entity identified as “Sizmek” in the GDPR Addendum.

Data subjects

Data subjects are described in Schedule A to the GDPR Addendum.

Categories of data

The personal data is described in Schedule A of the GDPR Addendum.

Processing operations

The personal data transferred will be subject to the following basic processing activities: The processing operations are described in Schedule A of the GDPR Addendum.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures implemented by the data importer are as described in Schedule B to the GDPR Addendum.