

## **Data Processing Addendum to the Services Agreement**

between **Customer**

hereinafter also referred to as “**(Data) Controller**”

and

**Sizmek**

hereinafter also referred to as “**(Data) Processor**”

each referred to as a “**Party**”  
together referred to as the “**Parties**”

### **Preamble**

1. This Data Processing Addendum (“**DPA**”) is incorporated by reference into the Services Agreement and all related orders for Sizmek Services between Customer and the applicable Sizmek Contracting Entit(y/ies) set forth in the Services Agreement. This DPA applies to the extent that the applicable Data Protection Law applies to the processing of Personal Data pursuant to the Services Agreement.
2. This DPA is supplemental to the Services Agreement and sets out the terms that apply when Personal Data is processed by Sizmek under the Services Agreement. The purpose of the DPA is to ensure that such processing is conducted in accordance with applicable laws, including the Data Protection Law, 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 DPA details the Parties' rights and obligations related to the scope of the processing of Personal Data. Subject to paragraph 1 above, this DPA shall apply to all processing of Data Controller's Personal Data 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 DPA 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 DPA 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 DPA.
2. If a Customer entity has executed orders under the Services Agreement but is not a party to the Services Agreement, this DPA 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, and in accordance with any contractual requirements between Customer and Sizmek, permitting an Affiliate (defined below) to use the Services specified in a Services Agreement, that Customer Affiliate is a party to this DPA.
4. If a Customer enters into this DPA 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 DPA 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 party to both the Services Agreement and this DPA that uses the Services.

**Data Protection Law:** means, as applicable, the GDPR and any national implementing laws, regulations and secondary legislation pertaining thereto, as amended or updated from time to time, as may be applicable in the particular context. Any reference to the applicable law of the European Economic Area (the "EEA"), including the GDPR, that is directly applicable or directly effective in the United Kingdom at any time is a reference to such law as it applies in England and Wales from time to time including as retained, amended, extended, re-enacted or otherwise given effect on or after 11pm on the 31 of January 2020 (the "UK Data Protection Law").

**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 in connection with the Services.

**Services:** means the System and other services of Sizmek that process Personal Data and that are used by Customer pursuant to a Services Agreement, including for the delivery of digital advertisements to digital advertising media, measurement and data enablement, creative management and optimisation, media execution and reporting to create effective digital advertising 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, in respect of the Services Agreement, the applicable Sizmek Contracting Entity party to the Services Agreement, and in respect of the DPA, Amazon Europe Core S.à r.l. ("AEC").

**Sizmek Contracting Entities:** means the Sizmek (Amazon) entity(ies) party to the Services Agreement, AEC, or any of their applicable Affiliates.

**Standard Contractual Clauses:** means (i) in case of transfers of EEA Personal Data subject to the GDPR outside of the EEA, (x) for Services Agreements entered into on or after September 27, 2021, the standard contractual clauses promulgated pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "2021 EU Contractual Clauses"), as set forth in **Schedule C**, and (y) for Services Agreements entered into before September 27, 2021, 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 (the "EU Contractual Clauses"), as set forth in **Schedule D**; and (ii) in case of transfers of Personal Data subject to the UK Data Protection Law outside of the United Kingdom, the EU Contractual Clauses, as set forth in **Schedule D**.

## **Section 2**

### **Subject of the DPA (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 applicable Data Protection Law.
2. The Data Controller selected Sizmek as a service provider by exercising its duties of diligence under the applicable 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 DPA 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 applicable Data Protection Law.
4. Direction means the written instruction issued by the Data Controller to Sizmek, 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 applicable 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 may at any time issue supplementary directions regarding the purpose, manner and extent of the processing of the Personal Data. 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 or make other claims 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 Data Processor 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 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, the European Union, any member state thereof, or the United

Kingdom (“**Applicable Laws**”). Where the Data Processor is relying on Applicable Laws as the basis for processing Personal Data, the Data Processor will inform the Data Controller of the requirement before the processing required by 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 Data Subject requests provided for in the applicable Data Protection Law; (ii) in responding to requests, investigations or audits by an applicable Data Protection Law supervisory authority or regulator (a “**Data Protection Authority**”); and (iii) in complying with any request by Data Controller with respect to ensuring compliance with Data Controller’s obligations under the applicable Data Protection Law with respect to security, breach notifications, impact assessments and consultations with applicable Data Protection Authorities in connection with processing of Personal Data hereunder, provided that Data Processor shall (unless prohibited by Applicable Laws) notify Data Controller without undue delay should it receive any such request or query from a Data Subject or a Data Protection Authority if such request is identified to Data Processor as pertaining to the Personal Data of the Data Controller; provided further that this does not preclude the Data Processor from making tools available directly to Data Subjects that they may use to fulfil requests pertaining to their Personal Data (in which case no notification need be provided to Data Controller with respect to such requests);
  - 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 EEA 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](mailto:sizmek-legal@amazon.com).

## **Section 5 Subcontractors**

The Data Controller consents to the Data Processor using Affiliate and third-party sub-processors of Personal Data under this DPA. The Data Processor confirms that it has entered or (as the case may be) will enter with such sub-processors into a written agreement incorporating terms which are substantially similar to those set out in this DPA. 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**

1. The Standard Contractual Clauses will apply to Personal Data that is transferred outside the EEA 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 applicable Data Protection Law). The Standard Contractual Clauses will not apply (i) to Personal Data that is not transferred, either directly or via onward transfer, outside such territory or (ii) to the extent the Personal Data is transferred outside such territory pursuant to an alternative recognised compliance standard for the lawful transfer of personal data (as defined in the applicable Data Protection Law) or as part of a transfer that is otherwise not legally required to be subject to the Standard Contractual Clauses.

2. With respect to transfers of Personal Data at the direction of the Data Controller to other providers or third parties (i.e., onward transfers other than transfers to subprocessors of Sizmek for purpose of performing services on behalf of Sizmek), the Data Controller is solely responsible for entering into standard contractual clauses or obtaining other legally sufficient mechanism for transfer of the Personal Data to such third parties.

## **Section 8 Term of Addendum**

Except where this DPA expressly stipulates any surviving obligation, the term of this DPA shall commence upon the later of the effectiveness of (i) the applicable Services Agreement and (ii) the applicable Data Protection Law, and terminate upon termination or expiration of the Services Agreement.

## **Section 9 Miscellaneous**

1. Where GDPR is the applicable Data Protection Law, this DPA shall be governed by the laws of the Grand Duchy of Luxembourg.

2. This DPA 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 DPA accordingly.

3. In the event that individual provisions of this DPA are ineffective, the remaining provisions of the DPA 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 selected 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, to enable restoration of the Personal Data.

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 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, to prevent restoration of the Personal Data.

## SCHEDULE C

### 2021 EU CONTRACTUAL CLAUSES

#### SECTION I

##### *Clause 1*

##### **Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### *Clause 2*

##### **Effect and invariability of the Clauses**

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

##### *Clause 3*

##### **Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*  
**Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*  
**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*  
**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7*  
**Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

*Clause 8*  
**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to

understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

#### **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation,

or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.,

## 8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### *Clause 9*

## **Use of sub-processors**

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Clause 10*  
**Data subject rights**

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*  
**Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*  
**Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and,

where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*  
**Supervision**

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*Clause 14*  
**Local laws and practices affecting compliance with the Clauses**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices

not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 15*

### **Obligations of the data importer in case of access by public authorities**

#### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### *Clause 16*

#### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
- (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### *Clause 17*

#### **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Luxembourg.

### *Clause 18*

#### **Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Luxembourg.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

## APPENDIX

### ANNEX I

#### A. LIST OF PARTIES

Data exporter(s): Customer (as defined in the DPA).

Data importer(s): Sizmek (as defined in the DPA).

#### B. DESCRIPTION OF TRANSFER

Description: 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) (“Digital Properties”) 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 on Digital Properties, 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.

Data subjects: Users of Data Controller and third-party Digital Properties in connection with which Sizmek is used to deliver, measure, or manage advertising campaigns.

Special categories of personal data: N/A.

Frequency of the transfer: Continuous.

Duration of processing: As described in Services Agreement.

#### C. COMPETENT SUPERVISORY AUTHORITY

The National Commission for Data Protection (Commission Nationale pour la Protection des Données – CNPD).

## **ANNEX II**

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

See Schedule B of the DPA.

## SCHEDULE D

### EU 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 DPA)

(the “data **exporter**”)

and

Sizmek (as defined in the DPA)

(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<sup>1</sup>**

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:

---

<sup>1</sup> 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.

- (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 or 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 DPA.

### **Data importer**

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

### **Data subjects**

Data subjects are described in Schedule A to the DPA.

### **Categories of data**

The personal data is described in Schedule A of the DPA.

### **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 DPA.

## **APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

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 DPA.

## SCHEDULE E

This Schedule E applies solely to the extent the Customer is purchasing Services from Amazon (China) Holding Company (“**Amazon China**”) or is otherwise using the Services in advertising campaigns addressed to data subjects in the People’s Republic of China.

Solely to the extent described above, the following applies, notwithstanding anything to the contrary in the DPA or the Agreement:

1. The definition of “**Data Protection Law**” includes the Personal Information Protection Law of the People’s Republic of China (“**PIPL**”), to the extent applicable.
2. In respect of the DPA, “**Sizmek**” is defined as Amazon China to the extent PIPL is the applicable Data Protection Law.
3. “**Applicable Laws**” is defined to include the applicable laws of the People’s Republic of China, solely with respect to processing of Personal Data subject to PIPL.
4. Customer agrees that Personal Data may be transferred outside of the People’s Republic of China, and Customer is solely responsible for any notice or consent requirements (including with respect to Data Subjects) applicable to such transfers. Applicable standard contractual clauses for such transfers will be incorporated into the DPA when promulgated by the applicable Data Protection Authority.