DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") along with the Standard Contractual Clauses set forth in Annex 1 to this DPA ("SCCs") have been pre-signed on behalf of Affise. To complete this DPA and SCCs (if applicable), please fill in your details, sign in the relevant signature blocks and send the completed signed DPA and SCCs (if applicable) to Affise by email to privacy@affise.com. As an alternative, these documents can be filled in and signed via DocuSign.

In the course of the use of the Site and the Software offered through the Site by Affise under the Agreement, Affise may Process certain Personal Data on behalf of the Customer. If such Processing occurs, the Customer and Affise agree to comply with the terms and conditions set out in this DPA in connection with such Personal Data. The purpose of this DPA is to ensure such Processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data are processed.

For transfers of Personal Data from Affise to the Customer, when the Customer is located in a country that does not ensure an adequate level of data protection within the meaning of Data Protection Legislation, to the extent such transfers are subject to Data Protection Legislation, the SCCs apply as attached and incorporated herein and the Customer and Affise agree to sign SCCs and comply with the terms and conditions set out in the SCCs in connection with such transfers.The SCCs shall come into effect and be deemed executed upon execution of this DPA and shall apply pursuant to the order of precedence described in clause 9.2 of this DPA.

The DPA forms a part of the Terms and Conditions of Use found at https://affise.com/terms-and-conditions-of-use/, unless the Customer has entered into an End-User Agreement with Affise, in which case, it forms a part of such agreement (in either case, the "Agreement"). The Customer and Affise are hereinafter jointly referred to as the "Parties" and individually as the "Party". A party to this DPA is the Customer entity which has accepted the Terms and Conditions of Use and/or has entered into the End-User Agreement. If the Customer entity signing this DPA neither has accepted the Terms and Conditions of Use nor has entered into the End-User Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA. If the Customer has previously executed a data processing addendum with Affise, this DPA supersedes and replaces such prior data processing addendum.

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

Processing of the Personal Data by Affise in the framework of the Customer's use of the Software under the Agreement without execution of this DPA is not possible as it constitutes violation of Art. 28.3 of the GDPR.

1. DEFINITIONS

The following terms shall have the meanings ascribed to them herein.

1.1. **Affise**: The Affise entity which is a party to this DPA being Affise Technologies Ltd, a company incorporated under the laws of the Republic of Cyprus.

1.2. **Customer**: any person/business who uses the Software through the Site during a free trial period under the Terms and Conditions of Use and the Privacy Policy and/or after the free trial period having concluded/accepted the End-User Agreement.

1.3. **Data Protection Legislation**: the data protection or privacy laws in the European Union ("EU"), European Economic Area ("EEA") and their Member States, including the General Data Protection Regulation (the "GDPR") ((EU) 2016/679), and any successor legislation to the GDPR or the Data Protection Act 1998 when the GDPR is no longer directly applicable in the United Kingdom.

1.4. **Sub-processor**: any Processor engaged by or on behalf of Affise to Process the Personal Data on behalf of the Customer in connection with the Agreement.

1.5. The terms “Controller”, “Data Subject”, “Data Subject Right Request”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processor”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR.

2. COMPLIANCE

2.1. The Parties acknowledge and agree to comply with applicable Data Protection Legislation in relation to the Personal Data shared with Affise under the terms of this DPA and in the framework of Parties’ relations under the Agreement.

2.2. In its use of the Software and provision of instructions to Affise, the Customer shall Process the Personal Data in accordance with the requirements of applicable Data Protection Legislation. The Customer shall have sole responsibility for the accuracy, quality and legality of the Personal Data and the means by which the Customer acquired the Personal Data.

2.3. In relation to the Processing of the Personal Data, Affise acts on behalf of and on the instructions of the Customer in carrying out the purpose of Processing set out in clause 3.4 of this DPA.

2.4. This DPA and the Agreement are Customer’s complete and final instructions at the time of execution of the DPA for the Processing of the Personal Data. Any additional or alternate instructions must be agreed upon separately. The Processing described in clauses 2.3 and 3.4 of this DPA is deemed an instruction by the Customer to process the Personal Data.

3. DATA PROCESSING

3.1. The Parties acknowledge and agree that with regard to the Processing of the Personal Data, the Customer is the Controller, Affise is the Processor and that Affise will engage Sub-processors pursuant to the requirements set forth in section 6 of this DPA and the Data Protection Legislation.

3.2. **Subject matter of the Processing**. The subject matter of the Processing of the Personal Data is to ensure the Customer’s use of the Software through the Site, to enable the Customer to review and analyze data processing results via the Software and to exercise other rights as further described in the Agreement.

3.3. **Duration of the Processing**. The Processing shall last for the period during which the Customer has the right of access to and use of the Software and other rights under the Agreement (but not longer than the term of the Agreement), except as otherwise required by applicable law.

3.4. **Nature and purpose of the Processing**. Affise offers performance marketing software as a service solution through the Site. It allows to upload and download the data to and from the Software, to customize the built-in features and tools of the Software in order to retrieve, gather, process and analyze the Customer’s data as well as to review and analyze data processing results via the Software or by downloading the reports and data. In the framework of these activities the Processing of the Personal Data occurs upon the Customer’s instructions in accordance with the terms of the Agreement. The purpose of the Processing under this DPA is to perform Affise’s obligations under the Agreement and this DPA.

3.5. **Categories of Data Subjects**. On behalf of and on the instructions of the Customer Affise Processes the Personal Data in relation to the following Categories of Data Subjects:

Customer’s end-users (or end-users of the Customer’s clients) who use or interact with the Customer’s websites, products, services, advertisements and/or mobile application services (or websites, products, services, advertisements and/or mobile application services of the Customer’s clients).

3.6. **Types of the Personal Data** which may be Processed when using the Software. In relation to the Data Subjects identified in clause 3.5, Affise may Process on behalf of and on the instructions of the Customer the following Personal Data:

technical Identifiers: IP addresses of non-EEA end-users, cookie IDs, geodata (with city-level precision), digital fingerprints (including timestamped user agents) and custom unique user IDs ("ClickID");

engagement information: the information which refers to the Customer's ad campaigns and Data Subjects' actions (e.g. log files, clicks on the Customer's ads, ad impressions viewed, conversions registered and other interactions, events and actions the Customer chooses to measure and analyze within the Software).

3.7. For the purpose of clarity, the Customer shall not configure the Software to collect any data that is not permitted to be collected pursuant to the terms of the Agreement or that is beyond the scope identified above in this section 3 of this DPA.

4. OBLIGATIONS OF THE CUSTOMER

4.1. The Customer confirms:

4.1.1. it has the legal capacity to enter into and execute this DPA and it is a Controller which determines the purposes and means of the Processing of the Personal Data;

4.1.2. its instructions in connection with the processing of the Personal Data are in accordance with the Data Protection Legislation and will not cause Affise to breach the Data Protection Legislation. The Customer shall be solely responsible for the legality of the Personal Data and for ensuring it has consents of the Data Subjects mentioned in clause 3.5 to enable the collection and Processing of the Personal Data pursuant to the terms of the Agreement and this DPA;

4.1.3. it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Affise for Processing in accordance with the terms of the Agreement and this DPA.

4.2. The Customer may use information received in connection with clauses 5.5, 5.6 and 5.8 of this DPA only to assess Affise's compliance with the Data Protection Legislation and this DPA. The Customer must keep this information confidential, unless it is the Customer's confidential information.

4.3. If the Customer is an agency or network, it is obliged to instruct Affise (i) to keep the Personal Data relating to its clients (advertisers, brands, etc.) separate in the Software and (ii) in case the Customer terminates its relationship with the client, to cease the Processing of the Personal Data relating to the corresponding client, to delete it or make available for retrieval and delete existing copies, except as otherwise prohibited or allowed by any applicable law.

5. OBLIGATIONS OF AFFISE

5.1. Affise shall Process the Personal Data only on the Customer's lawful documented instructions, including Processing pursuant to section 3 of this DPA, unless compelled to by the EU or Member State law to which Affise is subject. In this case, Affise shall notify the Customer immediately.

5.2. Affise shall implement appropriate technical and organizational measures designed to protect the Personal Data against unauthorized processing, including unauthorized disclosure, access, destruction, loss and alteration, taking into account (i) the state of the art, (ii) costs of implementation, (iii) nature, scope, context and purposes of the Processing, as well as (iv) risks posed to Data Subjects.

5.3. Affise shall grant access to the Personal Data within its organization only to the personnel who require such access (i) in connection with their role and (ii) strictly for the purposes of performance of Affise's obligations under the Agreement.

5.4. Affise confirms that it has informed and instructed its personnel of the rules of Processing of the Personal Data under this DPA and guarantees that its personnel maintain confidentiality and security of the Personal Data.

5.5. Upon the Customer's written request, Affise shall make available information necessary to demonstrate compliance with the obligations laid down in the Data Protection Legislation and this DPA, provided

that (i) the requested information is in Affise's possession or control and (ii) the Customer has no other reasonable means of obtaining such information.

5.6. Upon the Customer's written request, Affise shall provide the Customer with information necessary to demonstrate Affise's compliance with this DPA in the form of (i) responses to a reasonable written questionnaire submitted by the Customer and/or (ii) inspection of documentation reasonably required to demonstrate Affise's compliance.

5.7. Affise shall adhere to clauses 5.5 and 5.6 only to the extent which is not contrary to the law and/or Affise's confidentiality obligations given to its partners or other customers.

5.8. At the request of the Customer as well as at the Customer's sole cost and expense, Affise shall allow for and contribute to audits, including inspections, related to Processing of the Personal Data under this DPA and conducted by the Customer or an auditor mandated by the Customer not more than once a year and solely for the purposes of meeting its audit requirements pursuant to applicable Data Protection Legislation. To request an audit, the Customer must submit a detailed audit plan at least one month prior to the proposed audit date describing the proposed scope, duration and start date of the audit. Audit requests must be sent to privacy@affise.com. The Customer or the auditor mandated by the Customer must execute a written confidentiality agreement acceptable to Affise before conducting the audit. The audit must be conducted during regular business hours, subject to Affise's policies, and may not unreasonably interfere with Affise's business activities. The Customer shall use (and ensure that each of its mandated auditor uses) its best efforts to avoid causing any damage, injury or disruption to Affise's premises, equipment, personnel and business while its (or auditor's) personnel is on those premises in the course of such an audit or inspection. Affise might deny access to its premises for the purposes of an audit or inspection stipulated by this clause 5.8 to (i) any individual unless he or she produces reasonable evidence or identity and authority, and (ii) any competitor of Affise.

5.9. Affise warrants that it will promptly notify the Customer regarding:

(i) any changes in the Laws which might affect Processing of the Personal Data provided for by this DPA,

(ii) any accidental or unauthorized access to the Personal Data Affise has received from the Customer,

(iii) any request received directly from the Data Subjects, including Data Subject Rights Requests, without responding to the request unless it has received prior written authorization to do so by the Customer,

(iv)any instruction of the Customer which, in Affise's opinion, infringes the GDPR or other EU or Member State data protection provisions.

5.10. If Processing or transfer of the Personal Data to a third country is required by the EU or Member State law to which Affise is subject (without documented instructions of the Customer), Affise shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

5.11. Taking into account the nature of Processing and the information available to Affise, Affise shall assist the Customer, in ensuring compliance with obligations pursuant to Art. 32 (Security of processing), Art. 33 (Notification of a personal data breach to the Supervisory Authority), Art. 34 (Communication of a personal data breach to the data subject), Art. 35 (Data protection impact assessment) and Art. 36 (Prior consultation) of the GDPR. For the avoidance of doubt, (i) if the Customer is required to do so under the Data Protection Legislation, Affise shall take reasonable measures to cooperate and assist the Customer in conducting a data protection impact assessment and related consultations with any Supervisory Authority to the extent the Customer does not otherwise have access to the relevant information and to the extent such information is available to Affise, at the Customer's expense, (ii) Affise shall notify the Customer without undue delay on becoming aware of a Personal Data Breach, provided that such breach is not caused by the Customer or Customer's personnel, and shall provide the Customer with information (to the extent in Affise's possession) to assist the Customer to meet any obligations to inform Data Subjects or Supervisory Authorities of the Personal Data Breach under the Data

Protection Legislation, (iii) Affise shall provide reasonable assistance to the Customer in the cooperation or prior consultation with the Supervisory Authority to the extent required under the GDPR;

5.12. Taking into account the nature of Processing, Affise shall assist the Customer, at the Customer's cost, by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights. The obligation of such assistance applies to Affise to the extent the Customer does not have access to the Personal Data necessary to respond to such requests through its access to and use of the Software. For the avoidance of doubt, the Customer is responsible for responding to Data Subject request for access, correction, restriction, objection, erasure or data portability of that Data Subject's Personal Data.

5.13. Affise (i) shall promptly notify the Customer if it receives a request from a Data Subject under any Data Protection Legislation in respect of the Customer's Personal Data (unless prohibited by applicable law), and (b) shall not respond to that request except on the documented instructions of the Customer or as required by applicable laws. Notwithstanding the foregoing, Affise shall be permitted to respond (including through automated responses) to any such requests informing the Data Subject that his/her request has been received and/or with instructions to contact the Customer in the event that his/her request relates to the Customer.

6. SUB-PROCESSING

6.1. The Customer hereby consents to Affise appointing those companies listed at https://affise.com/affise-data-subprocessors as third party processors of the Personal Data under this DPA ("Sub-processors").

6.2. Affise shall contractually impose on the Sub-processors the same data protection obligations as imposed on Affise under this DPA. Subject to clause 8.1 of this DPA, Affise shall remain fully liable to the Customer for the performance of the Sub-processors' obligations.

6.3. In case of engagement of a new Sub-processor or replacing already existing Sub-processor, Affise shall inform the Customer of any intended changes by updating its list of Sub-processors accessible under the link stated in clause 6.1 of this DPA and notifying the Customer in advance of the change via email or through the Customer's account in the Software. By doing so, Affise gives the Customer an opportunity to object to such changes. If, within 30 calendar days of receipt of that notice, the Customer objects in writing on reasonable grounds to the proposed changes, the Parties will work together to find a solution satisfying both Parties.

7. TERM OF THIS DPA AND OBLIGATIONS AFTER ITS TERMINATION/EXPIRATION

7.1. This DPA shall stay in force until the time when Processing of the Personal Data is no longer necessary in relation to the use of the Software under the Agreement. The term of this DPA shall not exceed the term of the Agreement.

7.2. Upon termination or expiration of the Agreement in accordance with the terms of the Agreement (including cases of expiration of trial period after which the Customer does not want to continue to access/use the Software subject to the terms and conditions of the End-User Agreement), Affise shall cease all Processing of the Customer's Personal Data and, at the Customer's choice, delete (or otherwise make unrecoverable and/or anonymized) or make available to the Customer for retrieval all relevant Customer's Personal Data in Affise's possession and delete existing copies, except as otherwise prohibited or allowed by any applicable law. Affise shall extend the protections of the Agreement and this DPA to any such Personal Data and limit any further Processing of such Personal Data to only those limited purposes that require the retention.

8. LIMITATION OF LIABILITY

8.1. Affise's aggregate liability, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of Affise means the aggregate liability of Affise under the Agreement and this DPA together. For the avoidance of doubt, Affise's total liability for all claims from the Customer arising out of or

related to the Agreement and this DPA shall apply in the aggregate for all claims under both the Agreement and this DPA established under the Agreement.

9. MISCELLANEOUS

9.1. Governing Law. This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of the Republic of Cyprus.

9.2. If there is a conflict between the Agreement and this DPA, the terms of this DPA shall control as it relates to Processing of the Customer's Personal Data. If there is a conflict between this DPA and SCCs (if applicable), the terms of the SCCs shall control.

9.3. Nothing within this DPA relieves the Parties of their own direct responsibilities and liabilities under the Data Protection Legislation.

9.4. Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

9.5. Notwithstanding anything to the contrary, the Parties hereby agree that this DPA shall be retroactively effective to the first day of the access and use of the Software in the event that (i) this DPA is signed later than the acceptance by the Customer of the Terms and Conditions of Use (for the free trial period) or the End-User Agreement (if the free trial period is omitted), and (ii) the Processing of the Personal Data specified in clause 3.6 of this DPA occurs in the framework of such access/use of the Software from the first day of the access and use of the Software under the Agreement. For the avoidance of doubt, the sub-clauses (i) and (ii) above in this clause 9.5 apply cumulatively.

The Parties' authorized signatories have duly executed this DPA which becomes a binding part of the Agreement with effect from the later date set out below:

On behalf of the Customer:	**On behalf of Affise Technologies Ltd:**
Customer Full Legal Name: _____	
Signatory Name: _____	Signatory Name: Anna Olympiou
Signatory Position: _____	Signatory Position: Director
Address: _____ _____ _____	Address: 49 dromos, 41, K. Polemidia 4152, Limassol Cyprus
Signature: _____	Signature: _____
Date: _____ 20__	Date: 01 March 2023

ANNEX 1: STANDARD CONTRACTUAL CLAUSES

Processor to Controller

This Annex is attached to and forms part of the Data Processing Addendum and applies for transfers of Personal Data from Affise to the Customer, only when the Customer is located in a country that does not ensure an adequate level of data protection within the meaning of Data Protection Legislation, to the extent such transfers are subject to Data Protection Legislation.

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) ([1]) 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) and Clause 8.3(b);

(iii) N/A

(iv) N/A

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18.

(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

Not used

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 exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data ([2]), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9
Use of sub-processors

NOT APPLICABLE

Clause 10
Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13
Supervision

NOT APPLICABLE

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

Clause 14
Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(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 ([3]);

(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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Cyprus.

Clause 18
Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of the Republic of Cyprus.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Affise Technologies Ltd

Address: 49 dromos, 41, K. Polemidia, 4152, Limassol, Cyprus

Contact person's name, position and contact details: Vladimir Pokidko, Data Protection Officer, privacy@affise.com.

Activities relevant to the data transferred under these Clauses: The data exporter grants the data importer an end-user license to access the Site and use the Software (performance marketing software solution) through the Site in accordance with the Agreement and the Terms and Conditions of Use.

Signature and date: _____ Anna Olympiou / Director

01 March 2023

Role (controller/processor): processor

Data importer(s):

Name:_____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses: The data exporter grants the data importer an end-user license to access the Site and use the Software (performance marketing software solution) through the Site in accordance with the Agreement and the Terms and Conditions of Use.

Signature and date: _____

_____ 20__

Role (controller/processor): controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

End-users who use or interact with the Customer's websites, products, services, advertisements and/or mobile application services (or websites, products, services, advertisements and/or mobile application services of the Customer's clients).

Categories of personal data transferred

Personal Data relating to the End Users provided to the data importer through the Software by the data exporter:

- technical Identifiers: IP addresses of non-EEA end-users, cookie IDs, geodata (with city-level precision), digital fingerprints (including timestamped user agents) and custom unique user IDs ("ClickID");
- engagement information: the information which refers to the Customer's ad campaigns and Data Subjects' actions (e.g. log files, clicks on the Customer's ads, ad impressions viewed, conversions registered and other interactions, events and actions the Customer chooses to measure and analyze within the Software).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal Data relating to the End Users may be transferred on a continuous basis until it is deleted in accordance with the DPA.

Nature of the processing

The data exporter will provide to the data importer the services in nature of the Software (access to and use of the performance marketing software solution).

Purpose(s) of the data transfer and further processing

The data exporter will provide to the data importer the services in nature of the Software (access to and use of the performance marketing software solution) and will collect and process the Personal Data relating to the End Users for the purpose of the Agreement's performance.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained until it is necessary for the data exporter to perform the rights and obligations arising from the Agreement and Terms and Conditions of Use.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

N/A

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] This includes whether the transfer and further processing 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 or offences.

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.