Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms an integral part of the RedTrack Terms of Use, available at https://www.RedTrack.com/terms-of-use/, the master service agreement or similar agreement (including any exhibits, appendices, annexes, terms, orders or policies referenced therein) ("**Agreement**"), entered into by and between **Customer** and **RedTrack** that governs Customer's use and RedTrack's provision of RedTrack's Services. Customer and RedTrack are hereinafter jointly referred to as the "**Parties**" and individually as the "**Party**". Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

Instructions

This Data Protection Addendum has been pre-signed on behalf of RedTrack. To complete this Addendum, please fill in your details and sign in the relevant signature blocks and send the completed and signed DPA to RedTrack by email to privacy@redtrack.io.

In all cases where a specific term in an Agreement incorporates the DPA into the Agreement by reference, the DPA shall be deemed executed upon execution of the Agreement and will be legally binding and made an integral part of the Agreement.

1. **Definitions**. In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings ascribed to them herein.

1.1. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "**Data Protection Laws**" means the data protection or privacy laws in the European Union ("**EU**"), European Economic Area ("**EEA**") and their Member States, including the GDPR.

1.3. "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.4. "**Standard Contractual Clauses**" means the contractual clauses established by the European Commission concerning the international transfer of Personal Data, as set out in Annex 2.

1.5. "**Sub Processor**" means any Processor appointed by or on behalf of RedTrack or any RedTrack Affiliate to Process Personal Data on behalf of the Customer in connection with the Agreement; and

1.6. The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

2. **Processing of Customer Personal Data.**

2.1. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and RedTrack is the Processor. RedTrack shall not Process Customer Personal Data other than on the

Customer's documented reasonable and customary instructions, as specified in the Agreement or this DPA, unless such Processing is required by applicable laws to which the RedTrack is subject.

2.2. Customer instructs RedTrack (and authorizes RedTrack to instruct each Sub Processor) to (i) Process Customer Personal Data in a manner consistent with the terms of the Agreement and this DPA; and (ii) transfer Customer Personal Data to any country or territory specified in the Agreement or if no such country or territory are specified then to any territory or country, all as reasonably necessary for the provision of the Services and consistent with the Agreement and Section 11 of this DPA.

2.3. Customer warrants and represents that its instructions to Process Personal Data shall at all times comply with Data Protection Laws. Customer shall be solely responsible for the legality of the Personal Data and for ensuring it has an appropriate lawful basis to enable the collection and Processing of Personal Data pursuant to the terms of the Agreement and this DPA.

2.4. Annex 1 sets forth the details of the Processing of Customer Personal Data, as required by article 28(3) of the GDPR (*Details of Processing of Customer Personal Data*). In no event shall Customer configure the Services to collect or cause RedTrack to Process Personal Data that is beyond the scope set forth in Annex 1, including, specifically any Restricted Data (as defined in the Agreement).

3. **RedTrack Personnel.** RedTrack shall take reasonable steps to ensure that access to the Customer Personal Data is limited on a need to know/access basis and that all RedTrack personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Customer's Personal Data.

4. **Security.** RedTrack shall, in relation to the Customer Personal Data, implement appropriate technical and organizational measures to ensure an appropriate level of security, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR. In assessing the appropriate level of security, RedTrack shall take into account the risks that are presented by Processing Person Data, in particular risks arising from a Personal Data Breach.

5. **Sub Processing**.

5.1. Customer authorizes RedTrack and each RedTrack Affiliate to appoint (and permit each Sub Processor appointed in accordance with this Section 5 to appoint) Sub Processors in accordance with this Section 5 and any restrictions in the Agreement.

5.2. The Sub Processors used by RedTrack are specified at: https://redtrack.io/gdpr/ ("**Sub Processors Website**").

5.3. RedTrack may appoint new Sub Processors at any time and shall update the Sub Processors Website upon such appointments. If a Customer wishes to receive notice of any new Sub Processors, it may request to receive such notice by subscribing at the Sub Processors Website. If, within ten (10) days of such notice, Customer notifies RedTrack in writing of any reasonable objections to the proposed appointment, RedTrack shall not utilize such Sub Processor to Process Customer Personal Data until reasonable steps have been taken to address the objections raised by Customer, and Customer has been provided with a reasonable written explanation of the steps taken. Where such steps are not sufficient to relieve Customer's reasonable objections then Customer or RedTrack may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub Processor, without bearing liability for such termination.

5.4. With respect to each Sub Processor, RedTrack shall: (a) take reasonable steps to ensure that the Sub Processor is committed to provide the level of protection for Personal Data required by the Agreement; (b) ensure that the arrangement between RedTrack and the Sub Processor is governed by a written contract, including terms which, to the extent applicable to the nature of services provided by the Sub Processor, offer a level of protection that, in all material respects, are consistent with the levels set out in this DPA and the Agreement; and

(c) remain fully liable to the Customer for the performance of the Sub Processor's data protection obligations where the Sub Processor fails to fulfill such obligations.

6. **Data Subject Rights**.

6.1. Customer shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g. for access, rectification or deletion of Customer Personal Data etc.). Taking into account the nature of the Processing, RedTrack shall reasonably assist Customer insofar as feasible, to fulfil Customer's said obligations with respect to such Data Subject requests, as applicable, at Customer's sole expense.

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

7. **Personal Data Breach**.

7.1. RedTrack shall notify Customer, without undue delay, upon RedTrack becoming aware of a Personal Data Breach affecting Customer Personal Data. In such an event, RedTrack shall provide Customer with information (to the extent in RedTrack's possession) to assist Customer to meet any obligations to inform Data Subjects or Data Protection authorities of the Personal Data Breach under the Data Protection Laws.

7.2. At the written request of the Customer, RedTrack shall reasonably cooperate with Customer and take such commercially reasonable steps, as are agreed by the Parties or necessary under Data Protection Laws, to assist in the investigation, mitigation and remediation of each such Personal Data Breach, at Customer's sole expense.

8. **Data Protection Impact Assessment and Prior Consultation**.

8.1. At the written request of the Customer, RedTrack and each RedTrack Affiliate shall provide reasonable assistance to Customer, at Customer's expense, with any data protection impact assessments or prior consultations with Supervising Authorities or other competent data privacy authorities, as required under any applicable Data Protection Laws. Such assistance shall be solely in relation to Processing of Customer Personal Data by the RedTrack.

9. **Deletion or return of Customer Personal Data**.

9.1. RedTrack shall return or make available to Customer the Personal Data per the terms of the Agreement, or if no such terms are provided then immediately prior to termination of the Agreement. Following termination of the Agreement, Personal Data shall be deleted or otherwise made unrecoverable and/or anonymized, other than such copies, as authorized under the Agreement or this DPA, or required, to be retained in accordance with applicable law and/or regulation.

10. **Audit Rights**

10.1. Subject to sections 10.2 and 10.3, RedTrack shall make available to Customer on request such information necessary to demonstrate compliance with this DPA and shall allow for, and contribute to, audits by a reputable auditor mandated by Customer in relation to the Processing of the Customer Personal Data by RedTrack.

10.2. To the extent RedTrack has undergone a third party independent audit based on SOC 2, Type II or similar standards, then any audit right arising pursuant to section 10.1 shall be first satisfied by providing Customer with a report of such audit. If Customer, for reasonable reasons, is not satisfied by the independent audit report then Customer may request that a reputable auditor perform an audit pursuant to section10.1 and subject to Section 10.3. If RedTrack does not agree to such additional audit or inspection, then the Customer shall have the right to terminate the Agreement with immediate effect.

10.3. Customer shall give RedTrack reasonable prior written notice of any audit or inspection to be conducted under Section 10.1 and shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing any damage, injury or disruption to RedTrack's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. All such audits shall be subject to the confidentiality obligations set forth in the Agreement. Customer and RedTrack shall mutually agree upon the scope, timing and duration of the audit or inspection in addition to any reimbursement of expenses for which Customer shall be responsible. Any such audits shall not occur more than once a year (except where required by law or due to a Personal Data Breach). Additionally, RedTrack need not give access to its premises for the purposes of such an audit or inspection: (a) to any individual unless he or she produces reasonable evidence of identity and authority; (b) to any competitor of RedTrack; or (c) outside RedTrack's normal business hours.

11. **Transfers** Any transfers of Personal Data under the Agreement from the EU, EEA, Member States and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws or which transfer is not otherwise governed by a framework approved by the European Commission (such as the EU-US and Switzerland-US Privacy Shield framework) to which RedTrack is officially certified, shall be subject to the Standard Contractual Clauses. The Standard Contractual Clauses shall come into effect and be deemed executed upon execution of this DPA and shall apply pursuant to the order of precedence described in the preceding sentence.

12. **General Terms**

12.1. **Agreement and Order of Precedence**. Nothing in this DPA reduces either Party's obligations under the Agreement in relation to the collection, use, processing and protection of Personal Data. Any claims brought under this DPA shall be subject to the terms of the Agreement including, without limitation, choice of jurisdiction, governing law and any liability limitations or exclusions. In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed

otherwise in writing and signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.2. **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.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the later date set out below.

Customer:

Company Name: _____

Signature: _____

Name: _____

Title: _____

Date: _____

Annex 1: Details Of Processing Of Customer Personal Data

This **Annex 1** includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data. The subject matter of the Processing of the Customer Personal Data is to provide attribution and analytics services, as are further described in the Agreement. The duration shall be for the period set forth in the Agreement.

The nature and purpose of the Processing of Customer Personal Data: rendering Services in the nature of an attribution and marketing analytics platform, as further detailed in the Agreement.
The types of Customer Personal Data to be Processed are as follows: The data types that may be processed when using the services:

- **"Technical Information**": this refers to technical information related to an End User's mobile device or computer, such as browser type, device type and model, CPU, system language, memory, OS version, Wi-Fi status, time stamp and zone, device motion parameters and carrier.

- "**Technical Identifiers**": this refers to various unique identifiers that generally only identify a computer, device, browser or Application. For example, IP address (which may also provide general location information), User agent, IDFA (identifier for advertisers), Android ID (in Android devices); Google Advertiser ID, Customer issued user ID and other similar unique identifiers.

- "**Engagement Information":** this refers to information relating to the Customer's ad campaigns and End User actions, such as: clicks on Customer ads, ad impressions viewed, audiences or segments to which an ad campaign is attributed, the type of ads and the webpage or Application from which such ads were displayed, the webpages on Customer's website visited by an End User, the URL from the referring website, downloads and installations of Applications, and other interactions, events and actions Customers choose to measure and analyze within their Application or website (e.g. add to cart, in-app purchases made, clicks, engagement time etc.).

- Any other data types explicitly agreed by the Parties under the Agreement.

For the purpose of clarity, Customer shall not configure the Services 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.

T**he categories of Data Subject to whom the Customer Personal Data relates are as follows:**
End users who use or interact with Customer's websites, products, services, advertisements and mobile application services.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to reflect any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

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

[*The gaps below are populated with details of the Customer or its relevant Affiliate:*]

Name of the data exporting organisation:

Address:

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation

.....
(the data **exporter**) And

Name of the data importing organisation: RedTrack Technologies LTD

Address: Spyrou Kyprianou, 38, CCS BUILDING, 2nd floor, Kato Polemidia, 4154, Limassol, Cyprus

e-mail: privacy@redtrack.io

Other information needed to identify the organisation: Not applicable.

(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.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

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;

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.

(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

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

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

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

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

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

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

On behalf of the data exporter:

[*Populated with details of, and deemed signed on behalf of, the data exporter:*]

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any): Signature.....

On behalf of the data importer:

Name: RedTrack Technologies LTD

Address: Spyrou Kyprianou, 38, CCS BUILDING, 2nd floor, Kato Polemidia, 4154, Limassol, Cyprus

Other information necessary in order for the contract to be binding (if any): Not applicable.

Signature.....

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is

Is the entity defined as Customer in the DPA.

Data importer

The data importer is:

RedTrack Technologies LTD

Data subjects

The personal data transferred concern the following categories of data subjects:

As set forth in Appendix 1 of the DPA

Categories of data

As set forth in Appendix 1 of the DPA.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

It is not intended that RedTrack receive any special categories of data.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

collection, recording, organisation, structuring, storage, deletion, aggregation, analyzation, anonymization and pseudonymization in order to provide analysis services as described in the Agreement.

DATA EXPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data exporter:*]

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: RedTrack Technologies LTD

Authorised Signature .....

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Access Controls: Administrative access to our production environment is limited to a restricted number of individuals. Access to additional individuals is given only in extreme circumstances, for a specific purpose, and is limited in duration. Such access to these additional individuals is given only after the explicit approval of the security team User access is based upon termination and evaluated on a quarterly basis.

Physical and Environmental Security: General access to the office is controlled by the use of a card access system. Cameras are installed throughout the sites. Access to controlled areas is restricted through the use of card access and/or additional verification. All individuals without authorized access to the controlled areas must sign in and be escorted by an individual with approved controlled area access.

Application Security: Data importer has developed and implemented a strict, secure development program, based on Open Web Application Security Project (OWASP), and Microsoft Security Development Lifecycle. From the earliest phases of product design and planning, the security team takes an active role in how our products are built. Following completion, sensitive product developments are tested to ensure that application security has been thoroughly and properly addressed

Vulnerability monitoring through penetration testing: Data importer performs at least two annual Information Security penetration tests, which are conducted by accredited and completely independent information security companies. Vulnerabilities, if found, are addressed as part of our Risk Management Policy. RedTrack performs vulnerability assessment scanning using third-party tools at least twice a month, and after any major infrastructure change in our production environment

Data transfer security: Data transferred to data importer through its services are encrypted in transit by default on all supporting browsers. In addition, data recorded on HTTPS pages is fully encrypted and transferred to servers over a TLS connection

Networks security: RedTrack implements multiple and varied infrastructure security measures to protect customer information from unauthorized access, loss, alteration, viruses, Trojans and other similar harmful code. This includes: • Swift and regular updates of operating systems, hardware, and any third party software to avoid security vulnerabilities. Critical updates are deployed within one week from release on corporate as well as production systems. • Use of firewalls and Intrusion Prevention Systems (IPS) systems to limit access and protect RedTrack servers. • Hardening of all external-facing servers according to industry best practices. • Implementing anti-malware controls to prevent entry of malicious software. • Securing remote access communication using multifactor authentication. • Backing up customer data on a daily basis, on a rotating schedule.