Last Updated: January 9, 2019

This Data Processing Agreement (the "DPA"), entered into by the Optmyzr Customer identified on the applicable Optmyzr ordering document for Optmyzr services ("Customer") and Optmyzr, Inc. ("Optmyzr"), governs the processing of personal data that Customer uploads or otherwise provides Optmyzr in connection with the services, the processing of data by Optmyzr on behalf of Customer in connection with the services, and the processing of any personal data that Optmyzr uploads or otherwise provides to Customer in connection with the services.

Optmyzr offers online services and software (the "**Services**") through the URL: optmyzr.com which allows Customer to create and build marketing campaigns, optimize campaigns, and share automated reports. Customer has already signed up for the Service and agreed to Optmyzr's Terms of Use and Privacy Policy (collectively, the "**Agreement**"). This DPA is incorporated into the Agreement by reference. Collectively, the DPA (including the SCCs, as defined herein), the Agreement, and any applicable ordering documents are referred to in this DPA as the "**Optmyzr Agreement**." In the event of any conflict or inconsistency between any of the terms of the Optmyzr Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) the SCCs; (b) this DPA; (c) the Agreement; and (d) the applicable ordering document to the Optmyzr Agreement. Except as specifically amended in this DPA, the Optmyzr Agreement and applicable ordering document remain unchanged and in full force and effect.

1. **Definitions**.

1.1 The following definitions and rules of interpretation apply in this DPA.

"**Authorized Persons**" means the persons or categories of persons that the Customer authorizes to give Optmyzr Personal Data processing instructions.

"**Business Purpose**" means the services described in the Master Agreement or any other purpose specifically identified in Appendix A.

"**Controller-to-Controller SCCs**" means the Standard Contractual Clauses (Controller to Controller Transfers – Set II) in the Annex to the European Commission Decision of December 27, 2004, as may be amended or replaced from time to time by the European Commission.

"Controller-to-Processor SCCs" means the Standard Contractual Clauses (Processors) in the Annex to the European Commission Decision of February 5, 2010, as may be amended or replaced from time to time by the European Commission.

"**Customer Personal Data**" means (a) Personal Data that Customer uploads or otherwise provides Optmyzr in connection with Customer's use of Optmyzr's Services or for which Customer is otherwise a data controller or (b) the relevant Privacy and Data Protection Requirements otherwise defined as protected personal data.

"**Data Exporter**" means the controller who transfers the Personal Data.

"**Data Importer**" means the processor who agrees to receive from the Data Exporter Personal Data intended for processing on its behalf after the transfer in accordance with its 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.

"Data Protection Requirements" means the General Data Protection Regulation, Local Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy, data security, consumer protection, marketing, promotion, and text messaging, email, and other communications; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"**Data Subject**" means an individual who is the subject of Personal Data.

"European Personal Data" means Personal Data the sharing of which pursuant to this Agreement is regulated by the General Data Protection Regulation or Local Data Protection Laws.

"General Data Protection Regulation" means Regulation (EU) 2016/679 of the European Parliament and of the Council.

"Personal Data" means information about an individual that (a) can be used to identify, contact or locate a specific individual, including data that Customer chooses to provide to Optmyzr from services such as customer-relationships management (CRM) services; (b) can be combined with other information that can be used to identify, contact or locate a specific individual; or (c) is defined as "personal data" or "Personal Data" by applicable laws or regulations relating to the collection, use, storage or disclosure of information about an identifiable individual.

"**Processing**," "**processes**," or "**process**" means any activity that involves the use of Personal Data or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

"**Privacy and Data Protection Requirements**" means all applicable federal, state, and foreign laws and regulations relating to the processing, protection, or privacy of the Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

"**Security Breach**" means any act or omission that compromises the security, confidentiality, or integrity of Data or the physical, technical, administrative, or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure, or acquisition of Personal Data is a Security Breach whether or not the incident rises to the level of a security breach under the Privacy and Data Protection Requirements.

"SCCs" means all Controller-to-Processor SCCs and Controller-to-Controller SCCs entered into between the parties under the Optmyzr Agreement.

"Sub-processor" means any entity which provides processing services to Optmyzr in furtherance of Optmyzr's processing on Customer's behalf.

"Supervisory Authority" means an independent public authority which is (i) established by a European Union member state pursuant to Article 51 of the General Data Protection Regulation; or (ii) the public authority governing data protection, which has Supervisory Authority and jurisdiction over Customer.

1.2 This DPA is subject to the terms of the Optmyzr Agreement and is incorporated into the Optmyzr Agreement. Interpretations and defined terms set forth in the Optmyzr Agreement apply to the interpretation of this DPA.

1.3 The Appendices form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Appendices.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Appendices, the provision in the body of this DPA will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Appendices, the provision contained in the Appendices will prevail;

(c) any of the provisions of this DPA and the provisions of the Optmyzr Agreement, the provisions of this DPA will prevail; and

(d) any of the provisions of this DPA and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

2. **Personal Data Types and Processing Purposes**.

2.1 Customer retains control of its Personal Data and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Optmyzr.

2.2 Appendix A contains the categories of Personal Data processed and the categories of Data Subjects subject to this DPA.

3 **Compliance with Laws**.

The parties shall each comply with their respective obligations under all applicable Data Protection Requirements.

4 **Optmyzr's Obligations**.

4.1 Optmyzr will Process Customer Personal Data (i) only for the purpose of providing, supporting and improving Optmyzr's services (including to provide insights and other reporting), using appropriate technical and organizational security measures; and (ii) in compliance with the instructions received from Customer. Optmyzr will not use or process the Customer Personal Data for any other purpose. Optmyzr will promptly inform Customer in writing if it cannot comply with the requirements under Clauses 9-11, 13-16 of this DPA, in which case Customer may terminate the Optmyzr Agreement or take any other reasonable action, including suspending data processing operations. Optmyzr will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Privacy and Data Protection Requirements. Optmyzr must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Privacy and Data Protection Requirements.

4.2 Optmyzr will promptly comply with any Customer request or instruction from Authorized Persons requiring Optmyzr to amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized Processing.

4.3 Optmyzr will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless Customer or this DPA specifically authorizes the disclosure, or as required by law. If a law requires Optmyzr to Process or disclose Personal Data, Optmyzr must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

4.4 Optmyzr will reasonably assist the Customer with meeting the Customer's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of Optmyzr's Processing and the information available to Optmyzr.

4.5 Optmyzr will inform Customer promptly if, in Optmyzr's opinion, an instruction from Customer violates applicable Data Protection Requirements.

4.6 If Optmyzr is collecting Customer Personal Data from individuals on behalf of Customer, follow Customer's instructions regarding such Customer Personal Data collection (including with regard to the provision of notice and exercise of choice.

4.7 Optmyzr will promptly notify the Customer of any changes to Privacy and Data Protection Requirements that may adversely affect Optmyzr's performance of the Optmyzr Agreement.

4.8 The Customer acknowledges that Optmyzr is under no duty to investigate the completeness, accuracy, or sufficiency of any specific Customer instructions from Authorized Persons or the Personal Data other than as required under the Privacy and Data Protection Requirements.

4.9 Optmyzr will only collect Personal Data for the Customer using a notice or method that the Customer specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of the Customer's identity, the purpose or purposes for which their Personal Data will be processed, and any other information that is required by applicable Privacy and Data Protection Requirements. Optmyzr will not modify or alter the notice in any way without the Customer's prior written consent.

4.10 Upon request, Optmyzr will provide Customer with a summary of Optmyzr's privacy and security policies.

5 **Optmyzr's Employees**.

5.1 Optmyzr will limit Personal Data access to:

(a) those employees who require Personal Data access to meet Optmyzr's obligations under this DPA and the Optmyzr Agreement; and

(b) the part or parts of the Personal Data that those employees strictly require for the performance of duties.

5.2 Optmyzr will take commercially reasonable steps to ensure that employees and Sub-processors:

(a) are informed of the Personal Data's confidential nature and use restrictions;

(b) have received training on the Privacy and Data Protection Requirements relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware both of Optmyzr's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPA.

5.3 Optmyzr will take commercially reasonable steps to ensure the reliability, integrity, and trustworthiness of all of Optmyzr's employees and Sub-processors with access to the Personal Data.

6 **Customer Obligations**.

6.1 Customer agrees to:

(a) determine the purposes and general means of Optmyzr's processing of Customer's Personal Data in accordance with the Optmyzr Agreement; and

(b) comply with its protection, security and other obligations with respect to Customer Personal Data prescribed by Data Protection Requirements for data controllers.

6.2 Customer agrees to, at Optmyzr's request, designate to Optmyzr a single point of contact (the "**Authorized Agent**") responsible for (i) receiving and responding to Data Subject requests Optmyzr receives from Customer Data Subjects relating to Customer Personal Data; and (ii) notifying Optmyzr of Customer's intended response to a Data Subjects request relating to the access to or the rectification, erasure, restriction, portability, blocking or deletion of Customer Personal Data that Optmyzr processes for Customer, and authorizing Optmyzr to fulfill such responses on behalf of Customer.

7 **Controller-To-Controller Scenarios**.

Each party will, to the extent that it, along with the other party, acts as data controller, as the term is defined in applicable Data Protection Requirements, with respect to Personal Data, reasonably cooperate with the other party to enable the exercise of data protection rights as set forth in the General Data Protection Regulation and in other Data Protection Requirements. Where both parties each act as data controller with respect to Personal Data, and the transfer of data between the parties results in a transfer of European Personal Data to a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, each party agrees it will (a) provide at least the same level of privacy protection for European Personal Data as required under the U.S.-EU and U.S.-Swiss Privacy Shield frameworks; or (b) use the Controller-to-Controller SCCs, which are incorporated herein by reference. If data transfers under this DPA rely on Controller-to-Controller SCCs to enable the lawful transfer of Personal Data, as set forth in the preceding sentence, the parties agree that the following terms apply: (i) Data Subjects for whom a Customer processes European Personal Data are third-party beneficiaries under the Controller-to-Controller SCCs; (ii) Appendix A to this DPA shall apply as Annex B of the Controller-to-Controller SCCs; and (iii) for purpose of Clause II(h), the Data Importer will process the European Personal Data, at its option, in accordance with "the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the Data Importer complies with the relevant provisions of such an authorization or decision and is based in a country to which such an authorization or decision pertains, but is not covered by such authorization or decision for the purposes of the transfer(s) of the personal data." The parties acknowledge and agree that each is acting independently as Data Controller with respect of Personal Data and the parties are not joint controllers as defined in the General Data Protection Regulation.

8 **Third Party Data Processors**.

Customer acknowledges that in the provision of some services (such as CRMs), Optmyzr, on receipt of instructions from Customer, may transfer Customer Personal Data to and otherwise interact with third party data processors. Customer agrees that if and to the extent such transfers occur, Customer is responsible for entering into separate contractual arrangements with such

third party data processors binding them to comply with obligations in accordance with Data Protection Requirements. Such third party data processors are not Sub-processors.

9 **Security**.

9.1 Optmyzr will at all times implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, or damage, including, but not limited to, measures with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption of Customer Personal Data while in transit and at rest, as set forth in further detail in Appendix B. Optmyzr will document those measures in writing and periodically review them, at least annually, to ensure they remain current and complete.

9.2 Optmyzr will notify Customer without undue delay, and in any event within 48 hours of becoming aware of any breach of Personal Data.

9.3 Optmyzr will take commercially reasonable precautions to preserve the integrity of any Personal Data it processes and to prevent any corruption or loss of the Personal Data, including but not limited to establishing effective back-up and data restoration procedures.

10 **Security Breaches and Personal Data Loss**.

10.1 Optmyzr will promptly notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. Optmyzr will restore such Personal Data at its own expense.

10.2 Optmyzr will notify the other party if it becomes aware of:

(a) any unauthorized or unlawful processing of Customer's Personal Data; or

(b) any Security Breach.

10.3 Immediately following any unauthorized or unlawful Personal Data processing or Security Breach, the parties will co-ordinate with each other to investigate the matter. Optmyzr will reasonably co-operate with the Customer in the Customer's handling of the matter, including:

(a) assisting with any investigation;

(b) providing Customer with physical access to any facilities and operations affected; and

(c) making available all relevant records, logs, files, data reporting, and other materials required to comply with all Privacy and Data Protection Requirements or as otherwise reasonably required by the Customer.

10.4 Optmyzr will not inform any third party of any Security Breach without first obtaining the Customer's prior written consent, except when law or regulation requires it.

10.5 Optmyzr agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

10.6 Optmyzr will cover all reasonable expenses associated with the performance of the obligations under Clause 10.2 and Clause 10.3, unless the matter arose from the Customer's specific instructions, negligence, willful default, or breach of this DPA, in which case the Customer will cover all reasonable expenses.

6.7 Optmyzr will also reimburse Customer for actual reasonable expenses Customer incurs when responding to and mitigating damages, to the extent that Optmyzr caused a Security Breach, including all costs of notice and any remedy as set out in Clause 10.5.

11 **Cross-Border Transfers of Personal Data**.

11.1 If the Privacy and Data Protection Requirements restrict cross-border Personal Data transfers, the Customer will only transfer that Personal Data to Optmyzr under the following conditions:

11.2 If any Personal Data transfer between Optmyzr and Customer requires execution of Standard Contractual Clauses in order to comply with the Privacy and Data Protection Requirements, the parties will complete all relevant details in, and execute, the Standard Contractual Clauses as referenced herein above, and take all other actions required to legitimize the transfer, including, if necessary:

(a) co-operating to register the Standard Contractual Clauses with any Supervisory Authority in any European Economic Area country;

(b) procuring approval from any such Supervisory Authority; or

(c) providing additional information about the transfer to such Supervisory Authority.

11.3 Optmyzr will not transfer any Personal Information to another country unless the transfer complies with the Privacy and Data Protection Requirements.

12 **Term and Termination**.

12.1 This DPA will remain in full force and effect so long as:

(a) the Master Agreement remains in effect; or

(b) Optmyzr retains any Personal Information related to the Master Agreement in its possession or control (the "**Term**").

12.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Optmyzr Agreement in order to protect Personal Data will remain in full force and effect.

12.3 Optmyzr's failure to comply with the terms of this DPA is a material breach of the Optmyzr Agreement. In such event, Customer may terminate any part of the Optmyzr Agreement authorizing the processing of Personal Information effective immediately upon written notice to Optmyzr without further liability or obligation.

12.4 If a change in any Privacy and Data Protection Requirement prevents either party from fulfilling all or part of its Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Privacy and Data Protection Requirement within thirty (30) business days, they may terminate the Optmyzr Agreement upon written notice to the other party.

13 **Data Return and Destruction**.

13.1 The parties agree that on the termination of the data processing services or upon Customer's reasonable request, Optmyzr will, and will cause any Sub-processors to, at the request of Customer, return all of Customer's Personal Data and copies of such data to Customer in its possession or control in the format and on the media reasonably specified by the Customer or securely destroy such Personal Data and demonstrate to the satisfaction of Customer that it has taken such measures, unless Data Protection Requirements prevent Optmyzr from returning or destroying all or part of the Customer Personal Data disclosed. In such case, Optmyzr agrees to preserve the confidentiality of the Customer Personal Data retained by it and that it will only actively process such Customer Personal Data after such date in order to comply with applicable laws.

13.2 If any law, regulation, or government or regulatory body requires Optmyzr to retain any documents or materials that Optmyzr would otherwise be required to return or destroy, it will notify Customer in writing of that retention requirement, giving details of the documents or

materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. Optmyzr may only use this retained Personal Information for the required retention reason or audit purposes.

13.3 Optmyzr may continue to process Customer Personal Data that has been aggregated in a manner that does not identify individuals or customers to improve Optmyzr's systems and services.

14 **Notice to Customer**. Optmyzr will inform Customer if Optmyzr becomes aware of:

(a) Any non-compliance by Optmyzr or its employees with Clauses 9-11, 13-16 of this DPA or the Data Protection Requirements relating to the protection of Customer Personal Data processed under this DPA;

(b) Any legally binding request for disclosure of Customer Personal Data by a law enforcement authority, unless Optmyzr is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;

(c) Any notice, inquiry or investigation by a Supervisory Authority with respect to Customer Personal Data; or

(d) Any complaint or request (in particular, requests for access to rectification, erasure, restriction, portability, blocking or deletion of Customer Personal Data) received directly from Data Subjects of Customer. Optmyzr will not respond to any such request without Customer's prior written authorization.

15 **Records**.

15.1 Optmyzr will keep accurate and up-to-date records regarding any processing of Personal Data it carries out for the Customer, including but not limited to, the access, control, and security of the Persona Data, approved Sub-processors and affiliates, the processing purposes, and any other records required by the applicable Privacy and Data Protection Requirements (the "**Records**").

15.2 Optmyzr will ensure that the Records are sufficient to enable the Customer to verify Optmyzr's compliance with its obligations under this DPA.

16 **Audit, Certification**.

16.1 **Supervisory Authority Audit.** If a Supervisory Authority requires an audit of the data processing facilities from which Optmyzr processes Customer Personal Data in order to ascertain or monitor Customer's compliance with Data Protection Requirements, Optmyzr will cooperate with such audit. Customer is responsible for all costs and fees related to such audit, including all

reasonable costs and fees for any and all time Optmyzr expends for any such audit, in addition to the rates for services performed by Optmyzr.

16.2 **Audits.** Optmyzr will provide to Customer each year an opinion or Service Organization Control report provided by an accredited, third-party audit firm under the Statement on Standards for Attestation Engagements (SSAE) No. 18 ("**SSAE 18**") (Reporting on Controls at a Service Organization) or the International Standard on Assurance Engagements (ISAE) 3402 ("**ISAE 3402**") (Assurance Reports on Controls at a Service Organization) standards applicable to the services under the Optmyzr Agreement (each such report, a "**Report**"). If a Report does not provide, in Customer's reasonable judgment, sufficient information to confirm Optmyzr's compliance with the terms of this DPA, then Customer or an accredited third-party audit firm agreed to by both Customer and Optmyzr may audit Optmyzr's compliance with the terms of this DPA during regular business hours, with reasonable advance notice to Optmyzr and subject to reasonable confidentiality procedures. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Optmyzr expends for any such audit, in addition to the rates for services performed by Optmyzr. Before the commencement of any such audit, Customer and Optmyzr shall mutually agree upon the scope, timing, and duration of the audit. Customer shall promptly notify Optmyzr with information regarding any non-compliance discovered during the course of an audit. Customer may not audit Optmyzr more than once annually.

17 **Warranties**.

17.1 Optmyzr warrants and represents that:

(a) its employees, Sub-processors, agents, and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Privacy and Data Protection Requirements relating to the Personal Data; an

(b) it and anyone operating on its behalf will process the Personal Data in compliance with both the terms of this DPA and all applicable Privacy and Data Protection Requirements and other laws, enactments, regulations, orders, standards, and other similar instruments; and

(c) it has no reason to believe that any Privacy and Data Protection Requirements prevent it from providing any of the Optmyzr Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take reasonable appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

    (i) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction, or damage; and

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Privacy and Data Protection Requirement and its information and security policies, including the security measures required in Clause 10.1.

17.2 The Customer warrants and represents that Optmyzr's expected use of the Personal Data for the Business Purpose and as specifically instructed by the Customer will comply with all Privacy and Data Protection Requirements.

18 **Indemnification**.

18.1 Optmyzr agrees to indemnify, keep indemnified, and defend at its own expense the Customer against all costs, claims, damages, or expenses incurred by the Customer or for which the Customer may become liable due to any failure by Optmyzr or its employees, Sub-processors, or agents to comply with any of its obligations under this DPA or applicable Privacy and Data Protection Requirements.

18.2 Any limitation of liability set forth in the Optmyzr Agreement will not apply to this DPA's indemnity or reimbursement obligations.

19 Mediation and Jurisdiction.

19.1 Customer agrees that if the Data Subject invokes against it claims for compensation of damages under the Clauses, Optmyzr will accept the decision of the Data Subject:

(i) to refer the dispute to mediation, by an independent person or, where applicable, by the Supervisory Authority;

(ii) to refer the dispute to the courts in the Member State in which the Customer is established.

19.2 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 and international law.

20 **Governing Law, Jurisdiction, and Venue**.

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

21. **Variation of Contract**.

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

APPENDIX A
PERSONAL DATA PROCESSING PURPOSES AND DETAILS

1. Business Purposes. To facilitate Customer's use of the Optmyzr Services.

2. Data Subjects. The Personal Data transferred concerns the following categories of Data Subjects:

Depending on the services used by the Data Exporter:

- Google Ads, Bing Ads, Facebook Ads, Amazon Ads, sales and marketing leads of the Data Exporter; and
- Third parties that have, or may have, a commercial relationship with the Data Exporter (e.g. advertisers, customers, corporate subscribers and contractors).

3. Purposes of the Transfer. The transfer is made for the following purposes:

The transfer is intended to enable the Data Exporter to determine the purposes and means of the processing of personal data obtained through Data Importer's products to support the sales, marketing, or other business practices of the Data Exporter.

4. Categories of Data. The Personal Data transferred concerns the following categories of data:

The data transferred is the Personal Data provided by the Data Exporter to the Data Importer in connection with its use of Optmyzr's services, referred to as Customer Personal Data in the Agreement. Such Personal Data may include first name, last name, email address, contact information, CRM data concerning sales leads and customer lists, purchase history, prospective customers and clients, employees, and any notes provided by the Data Exporter regarding the foregoing.

5. Recipients. The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

Employees and other representatives of the Data Importer who have a legitimate business purpose for the processing of such personal data.

6. Sensitive Data (if appropriate). The personal data transferred concern the following categories of sensitive data:

None.

7. Data Protection Registration Information of Data Exporter (where applicable).

None.

8. Sub-processors.

Data Exporter consents to sub-processing by the following subcontractors:

- Techvitt Consultants LLP
- Optmyzr Tech IVS
- Techfruit Technologies Private Limited
- Asesorias EAP SpA

9. Additional Useful Information (storage limits and other relevant information).

The personal data transferred between the parties may only be retained for the period of time permitted under the Optmyzr Agreement. The parties agree that each party will, to the extent that it, along with the other party, acts as a data controller with respect to Personal Data, reasonably cooperate with the other party to enable the exercise of data protection rights as set forth in the Data Protection Requirements.

10. Basis for Receiving Personal Data with Cross-Border Restrictions

Optmyzr's legal basis for receiving Personal Data with cross-border transfer restrictions is that Optmyzr is EU-US Privacy Shield Certified.

Contact Information. Contact points for data protection enquiries:

Data Importer: Signatory to the DPA between the parties

Data Exporter: Signatory to the DPA between the parties

APPENDIX B
SECURITY MEASURES

REQUIRED TECHNICAL AND ORGANIZATIONAL DATA SECURITY MEASURES, SUCH AS:

- PHYSICAL ACCESS CONTROLS
    - Access to the premises where Optmyzr employees work is secured by at least one of the following: electronic key cards, video cameras, guard or alarms
- SYSTEM ACCESS CONTROLS.
    - Strong passwords are required for employees to access Optmyzr's business systems
    - Mobile devices used to access data are managed by Google's device policy and can be remotely disabled in case of loss
- DATA ACCESS CONTROLS.
    - Private data is restricted to employees who are working with a customer.
    - Access to accounts is logged.
- INTERNAL PROTOCOL & EDUCATION
    - Quarterly best practice sharing about data privacy
- ADDITIONAL SAFEGUARDS
    - Data is encrypted in transit
    - Transmissions of private data are exclusively over HTTPS
    - Data in the cloud is inside VPC (virtual private cloud)