

GDPR DATA PROCESSING ADDENDUM

(last updated: 15 October, 2024)

This Data Processing Addendum (“**DPA**”) supplements the Agreement or other written or electronic agreement, for the provision of services by Active Trail Ltd., a company registered under the laws of the state of Israel, registration number 513921072, of 48 Menachem Begin road, Tel Aviv, Israel, including its affiliates and/or subsidiaries (“**Company**”) and/or license to use its marketing automation product (“**Product**”) and any purchase orders thereunder as shall be issued by you or the entity you represent (“**Customer**”) from time to time (“**Agreement**”) between ,and is intended to set in writing the Parties' agreement in any matter relating to the Processing by Company of any Personal Data Controlled by the Customer as a Controller and inserted by Customer into the Product databases and/or otherwise as part of the Services and/or use of the Product.

All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement. This DPA shall govern any matter relating to Data Protection between the parties in any event of processing by Company of Personal Data controlled by Customer as a Controller, and in the event of any discrepancy or contradiction between anything said herein and in any other agreement between the Parties, including the Agreement, the provisions of this DPA shall prevail.

By signing this DPA, the Customer enters this DPA on behalf of itself and to the extent required by the Data Protection Laws and Regulations in the name and on behalf of the Authorized Affiliates, if and to the extent that Company processes Personal Data for which such Authorized Affiliates qualify as Controller. For purpose of this DPA Customer shall include Authorized Affiliates thereof.

The parties agree that the provisions of this DPA in themselves constitute written instructions from the Customer to the Company concerning the processing of Personal Data. The Company undertakes to process Personal Data in accordance with the instructions documented in this DPA, unless otherwise required by law.

How to execute this DPA:

- (i) This DPA has been pre-signed by Company.
- (ii) Annex A is an integral part of this DPA.
- (iii) Customer must send the signed DPA to Company’s email: dpo@activetrail.net.
- (iv) Upon confirmation of receipt of the validly signed DPA by Company to the aforementioned email address, the DPA will become legally binding (the “**Effective Date**”).

How this DPA applies:

- (i) If the Customer is a party to the Agreement (including by online acceptance of the Company's Terms of Use), this DPA is an addendum to and forms part of the Agreement.
- (ii) If Customer is not a party to the Agreement, this DPA is not valid and is not legally binding.

1. DEFINITIONS

- 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. "**Authorized Affiliate**" means any of Customer's Affiliate(s) which is permitted to use the Services pursuant to the Agreement but has not signed its own Agreement and is not a "Customer" as defined under this Agreement.
- 1.3. "**Controller**" means natural or legal person or an entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- 1.4. "**Data Breach**" means a breach of security of the services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed;
- 1.5. "**Data Protection Legislation**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Legislation.
- 1.6. "**Data Subject**" means an individual who is the subject of Personal Data.
- 1.7. "**EU Data Protection Legislation**" means Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"), or any other law or regulation which shall be applicable to EU Data Subjects at such time.
- 1.8. "**EU Model Clauses**" means the standard contractual clauses for Processors as approved by the European Commission pursuant to Decision C (2010)593, as they may be amended or replaced from time to time.
- 1.9. "**Personal Data**" means any information relating to an identified or identifiable natural person.
- 1.10. "**Sensitive Personal Data**" means (1) special categories of personal data as defined on Article 9 to the GDPR – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (2) financial information.
- 1.11. "**Process**" or "Processing" shall mean any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- 1.12. **"Processor"** means an entity that processes Personal Data on behalf of a Controller.
- 1.13. **"Services"** means any cloud service offering or customer support services provided by Company to Customer pursuant to the Agreement, including through the use of the Product.
- 1.14. **"Sub-Processor"** means any Processor engaged by Company or any of its affiliates, which processes Personal Data pursuant to the Agreement. Sub-Processors may include third parties or any Company affiliate.

2. Customer hereby declares that the EU Data Protection Legislation applies to it as either it is based within the EU and/or the database used in the Product and/or Services, and in which it is the Controller and in which Company shall be the Processor according to the Agreement, includes or may include Personal Data of Data Subjects in the EU.

3. Responsibilities

3.1 **Role of the Parties.**

Company shall Process Personal Data under the Agreement solely as a Processor acting on behalf of the Customer. Customer shall act as a Controller with respect to the Personal Data, and it shall be the sole owner of such database.

3.2 **Customer's Responsibilities and Representations.**

3.2.1 Customer represents that it has all rights and authorizations necessary for the Company to process Personal Data on its behalf pursuant to the Agreement.

3.2.2 In its use of the Services and Product, Customer will comply with its obligations under Data Protection Legislation in respect of its collecting and /or processing of Personal Data and any processing instructions it issues to the Company.

3.2.3 As Controller, Customer shall have sole responsibility for the accuracy, quality, reliability, integrity, legality and appropriateness of Personal Data, including the methods and consents Customer uses to acquire Personal Data.

3.2.4 Customer will respond to inquiries from Data Subjects and from applicable regulatory authorities concerning the Processing of the Personal Data, and will alert Company in writing of any inquiries from Data Subjects or from applicable regulatory authorities that relate to Company's Processing of the Personal Data, all according to the law and as further detailed hereunder. The Company will respond to such inquiries correspondingly to the Customer instructions, unless its required to comply with Company's legal obligations, dispute resolution and/or enforcement of Company's rights or agreements.

3.3 **Company's Responsibilities and Representations.**

3.3.1 Company will comply with any obligations applicable to it as a Processor under Data Protection Legislation and shall process Personal Data in accordance with the

Agreement. In the event that Company's opinion is that such instructions are in contradiction to Data Protection Legislation, Company shall notify the Customer.

3.3.2 At all times Company shall process Personal Data as confidential information. Company shall reveal such data without prior permission only when there is a reason to believe that the disclosure of this information is required by law, regulation subpoena, court order or other law enforcement related issues, agencies and/or authorities and/or to protect Company's rights, property or safety (including the enforcement of this DPA). In this case Company will notify Customer of such disclosure as soon as possible

3.3.3 Customer authorizes Company to Process Personal Data in the following ways: (1) in accordance with the Agreement, including any order forms, (2) in accordance with processes initiated by Customer through the use of the Service, including any customer support and (3) in accordance with commercially reasonable instructions provided by Customer, where instructions are consistent with the terms of the Agreement. The parties agree that an instruction shall be deemed to be given where Company acts within the framework of the Agreement including this DPA.

3.3.4 Data Breach. Company shall notify Customer within a maximum of 48 hours after becoming aware of a Data Breach and will use reasonable efforts to assist Customer in mitigating, where possible, the adverse effects of any such Data Breach. This notification shall be accompanied by any useful documentation to enable the data controller, if necessary, to notify this breach to the competent supervisory authority.

3.3.5 Return or Deletion of Customer Personal Data. Unless otherwise required by applicable Data Protection Legislation, the Company will destroy or return to Customer its databases containing Personal Data upon Customer's request, other than data that is required to comply with Company's legal obligations, dispute resolution and/or enforcement of Company's rights or agreements. Customer's data shall be erased or returned to Customer within 30 days on Customer's instruction. Company declares by writing, of the deletion of Customer's data at Customer's request. Company will be able to produce proof that the data has been destroyed.

3.4 Details of Personal Data and Processing Activities.

3.4.1 Subject matter. The subject matter of the processing under the Agreement is the Processing of Personal Data by Company as part of the provision of the Services and use of the Product according to the Agreement.

3.4.2 Duration. The duration of the processing under the Agreement is determined by the Agreement and its appendices and work orders.

3.4.3 Purpose. The purpose of the processing under the Agreement is the provision of the Services by the Company to Customer and use of the Product by the Customer, all as specified in the Agreement.

3.4.4 Nature of the Processing. The Company and/or its Sub-processors are providing Services or fulfilling contractual obligations to Customer as described in the Agreement. These Services may include the processing of Personal Data of Customer's Data Subjects by the Company and/or its Sub-Processors and accessing such data only for purpose of providing the Service.

3.4.5 Categories of Data Subjects. Customer's data subjects may include Customer's clients, potential clients, and other data subjects appearing on Customer's contact lists and stored on Company's products, as specified in **Annex A**.

3.4.6 Types of Personal Data. Personal Data that is submitted to the Services by the Customer and/or its users of the Product, and includes any information which Customer includes therein, as specified in **Annex A**. Despite of the aforementioned and as further detailed above it is hereby clarified that the Product is a marketing automation platform and therefore its databases are only intended to contain marketing contact details and the database security has been designed accordingly, and Customer must not insert any data which constitutes under GDPR special categories of personal data (also known as sensitive personal data) such as medical records or financial information.

4. **SUBPROCESSING**

4.1. **Appointment of Sub-Processors.** Customer grants Company and its affiliates a general authorization to engage or replace Sub-processors to perform parts of the Service, including customer support, provided that the conditions specified below are followed. Company and its affiliates may continue to use those Sub-Processors already engaged by them as of the date hereof, subject to the provisions hereunder. Customer may give written instruction to Company to be informed of any intended changes concerning the addition or replacement of Sub-Processors at least 30 days prior to their occurrence. In the event Customer objects to any such future change or addition of a Sub-Processor, it shall be entitled to object in writing, for instance by e-mail with return receipt, to Company within 20 days from receipt of Company's notification regarding such change, including detailed reasoning, and terminate the Agreement upon the coming into effect of such change or addition.

4.2 **Agreement with Sub-Processor.** Prior to receiving any Personal Data of Customer, Sub-Processors will engage with Company in written agreements that are substantially similar in scope, where applicable, to this DPA and the EU Model Clauses. Company and its affiliates shall ensure that each Sub-Processor performs the obligations under this DPA, as they apply to Processing of Customer Personal Data carried out by that Sub-Processor, as if it were party to this DPA in place of Company. Where Company's Sub-Processors fail to fulfill their data protection obligations, Company will remain responsible and liable for the performance of its obligations and of those Sub-Processors' obligations pursuant to this DPA.

5. **SECURITY MEASURES**

5.1 **Security Measures by Company.** Company will implement and maintain appropriate technical and organizational security measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data processed by it on behalf of Customer in the provision of the Services and/or use of the Product, taking into account the costs of implementation, the nature, scope, context, and purposes of the Processing, and the risk of varying likelihood and severity of harm to the Data Subjects. In assessing the appropriate level of security, Company shall weigh the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed ("Security Measures"). The Security Measures are subject to technical progress and

development. Company may update or modify the Security Measures from time to time. Despite of the aforementioned it is hereby clarified that the Security Measures implemented are not suitable to special categories of personal data (also known as sensitive personal data under GDPR) or financial information and Customer shall not include any such data in its databases Processed by Company.

5.2 Security Measures by Customer. Customer is responsible for using and configuring the Services in a manner which enables Customer to comply with Data Protection Legislation, including implementing appropriate technical and organizational measures.

5.3 Personnel

5.3.1 Confidentiality. Company shall guide personnel engaged in the Processing of Personal Data of the confidential nature of the Personal Data and provide appropriate training based on their responsibilities. Company shall execute written agreements with its staff to maintain the confidentiality of Personal Data, including following termination of their employment.

5.3.2 Access Control. Company shall use commercially reasonable efforts to limit access to Personal Data on a need to know basis.

5.3.3 DPO. If required by Data Protection Legislation, a Data Protection Officer shall be appointed by Company, and its contact details shall be provided upon request.

5.4 Sensitive Personal Data. Customer acknowledges and agrees that it must not submit to the Services / Product any Sensitive Personal Data (as such term is defined under the GDPR), nor shall it insert any financial information.

6. DPA's and Data Subjects' Rights

Company shall notify Customer if it receives a request from any applicable data protection authority, or a Data Subject for either access, correction, amendment or deletion of his/her Personal Data and/or any other exercise of its rights according to the Data Protection Legislation, and Company shall reasonably assist Customer on such request, if applicable. Company shall co-operate with data protection authorities according to Data Protection Legislation. Customer shall act according to the applicable Data Protection Legislation with regards to any such notice delivered to it by Company and shall respond to the Data Subject and edit the Personal Data accordingly. Company shall not respond to a Data Subject's message, unless required to do so by law. If applicable, Customer shall notify Company in writing of wrong details contained with the Personal Data, and if applicable, Company shall correct such details according to Customer's written instructions. Company shall act in accordance with the requirement of any Data Protection Legislation with regards to Data Subject's rights. All costs incurred by the Company with regards to its assistance to the Customer as detailed in this section 6 herein shall be borne by Customer.

7. Audit and Records

7.1 **Records.** Company shall keep records of all its Processing activities according to the requirements of Data Protection Legislation.

7.2. **Audit.** Company shall make available to the Customer, in accordance with Data Protection Legislation, such information in Company's possession or control as the Customer may reasonably request with a view to demonstrating Company's compliance with the obligations of data processors under Data Protection Legislation in relation to its processing of Personal Data.

8. DATA TRANSFERS AND EXPORTS

8.1 **Data Transfers.** Company may transfer and process Personal Data to and in other locations around the world where Company or its Sub-Processors maintain data processing operations as necessary to provide the Services as set forth in the Agreement.

8.2 **Data Transfers from the EU.** Where Personal Data is transferred from the European Union to Company affiliate or representative located in a country not recognized by the European Commission or the Swiss Federal Data Protection Authority as providing an adequate level of protection for Personal Data, Customer appoints Company to enter into the EU Model Clauses on Customer's behalf with such Company affiliate based outside of the EU and involved in the Processing of Personal Data, in the event Company determines such action is required according to Data Protection Legislation. In such event, Company will provide a copy of those EU Model Clauses to Customer upon Customer's written request.

8.3 If in the performance of this DPA Company transfers any Personal Data to a Sub-Processor located outside of the EU, Company shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, if required by Data Protection Legislation, such as: (a) the requirement for Company to execute or procure that the Sub-Processor execute to the benefit of the Customer standard contractual clauses approved by the EU authorities under EU Data Protection Legislation; (b) the requirement for the Sub-Processor to be certified under the EU-U.S. Data Privacy Framework; or (c) the existence of any other specifically approved safeguard for data transfers (as recognized under EU Data Protection Legislation) and/or a European Commission finding of adequacy.

9. DPIAs and Prior Consultations

To the extent required by Data Protection Legislation, Company will, upon reasonable written notice and at Customer's expense, provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments ("DPIAs") and/or prior consultations with data protection authorities.

10. Limitation of Liability

Each party's and all of its affiliates' liability, taken together in the aggregate, 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" under the Agreement, and any reference therein to the liability of a party means the aggregate liability of that party and all of its affiliates under the Agreement and this DPA. For the avoidance of doubt, Company and its affiliates' total liability for all claims from the Customer arising out of or related to the

Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and this DPA.

11. Governing Law

The parties agree that (1) governing law of this DPA, and (2) the forum for all disputes in respect of this DPA, shall be the same as set out in the Agreement, unless otherwise required by applicable Data Protection Legislation.

12. Term and Termination

This DPA shall become an integral part of the Agreement as stated in the preamble to this DPA and shall terminate upon the later of the termination of the Agreement or the final Process by Company of Personal Data controlled by Customer.

13. 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.

IN WITNESS WHEREOF, this DPA forms a binding part of the Agreement as described in the first page of this document as of the Effective Date. If this document has been electronically signed by either party such signature will have the same legal effect as hand written signature.

Processor:

Signature: _____

Active Trail Ltd.

By: _____

Title: _____

Date: _____

Controller:

Signature: _____

Customer: _____

By: _____

Title: _____

Date: _____

Annex A

This Annex A includes certain details of the Processing of Customer's Personal Data as required by Article 28(3) of the GDPR (or as applicable, equivalent provisions of any other Data Protection Legislation).

Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

Categories of Data Subjects: Customers and Customer's Client Data (data that the Customer insert to the Service as a Controller).

The types of Personal Data to be Processed: Customer may insert certain personal data to the Service. Personal data which are submitted to and/or included in the database / Services / Product by Customer, will be considered as Personal Data that the Customer has approved to Company to process in relation to the Agreement and this DPA. This may include the following types of personal data:

Customers: Identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);

Customer's Client Data: Identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address); personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data);.

Sensitive Data – Please note that, as further detailed in this DPA above, the submission to and/or inclusion in the database / Services / Product by Customer of any Sensitive Personal Data, as such term is defined under GDPR or financial information, is prohibited.