# ADDENDUM DATA CONTROLLER

APPOINTMENT OF DATA CONTROLLER
The User (hereinafter "Owner" or "Customer" or "Data Controller"),
by express acceptance of the Terms and Conditions of *reviewsmatter.io*
(hereinafter "Provider" or the "Data Processor"), accepts this addendum on the processing of personal data, which constitutes an integral part of the relationship between the Parties. This Addendum is signed pursuant to Article 28 of Regulation 679/2016 and governs the manner in which the Data Processor will process personal data on behalf of the Data Controller. Data Controller and Data Processor, may also be referred to individually as the "Party" and jointly as the "Parties".

WHEREAS.
-the processing operations of personal data carried out by the Data Controller are listed in the register of processing operations kept by the Data Controller;
-for some processing operations the Data Controller makes use of the cooperation of the Supplier;
-the Supplier, as part of the services offered to the Data Controller, as better detailed in the specific contract in place, may carry out personal data processing on behalf of the Data Controller;
-the Data Controller and the Provider have signed an agreement for the provision of an integrated web and tablet for creating, managing and sending review requests ("Service"), of which this document is an integral part;
-with reference to the Service made available by the Provider, the latter may process data personal data owned by the Controller and, more specifically, common data (first name, last name, contact details) of the Holder's end customers;
-the purpose of the processing is to provide a technological solution that allows the Holder to be able to take advantage of the Service;
-in accordance with Article 28.1 of Regulation (EU) 2016/679, General Data Protection Regulation (henceforth "GDPR"), "where a processing is to be carried out on behalf of the Controller of the Processing, the latter shall only use data controllers."
-the Data Controller has verified that the Provider, again pursuant to Article 28.1 of the GDPR, presents "sufficient guarantees to put in place appropriate technical and organizational measures so that the processing meets the requirements of the Regulation and ensures the protection of the rights of the data subject."
The Data Controller appoints the Provider as the "PERSONAL DATA PROCESSING RESPONSIBLE" (henceforth also simply "Processor" or "Processor"), with respect to the personal data that Supplier may process in the performance of its activities and those that may be entrusted to Supplier in the future.

In accordance with the GDPR, the activity performed by the Processor will be governed as follows:

1. DURATION. This appointment shall be effective for the duration of the Processor's relationship with the Controller and shall be deemed automatically revoked in the event of termination of the same.

2. PURPOSE OF THE PROCESSING. The data that are entrusted to the Manager, as part of the activities entrusted to him/her for the use of the Service, may be processed only for the purposes indicated in the mandate entrusted and/or in the contract entered into with the Owner. In particular, the data will be processed by the Provider only for the purpose of being able to guarantee the provision of the Service to the Owner who, in any case, will remain the only entity obliged to have to communicate to the end customer the purposes and obtain consent to the processing, as well as the communication of the data to third parties.

3. METHODS OF PROCESSING. The data may be processed on paper or digital media, depending on the activities carried out, provided that the tools are properly identified and inventoried by the Manager and systematically communicated to the Owner for his approval. In particular, the data will be processed by means of the *reviewsmatter.io* software platform.

4. DUTIES AND TASKS OF THE RESPONSIBLE PERSON. The Data Processor, as stipulated in Article 28 of the GDPR, undertakes to:

(a) process the entrusted personal data only on the documented instruction of the Controller, even in case of transfer of personal data to a third country, unless otherwise provided by law. In this case, the Responsible Party is still obliged to inform the Controller;

(b) ensure that the persons authorized to process have committed to confidentiality, or have an appropriate legal obligation of confidentiality. To this end, the Responsible Party to periodically verify that the persons in charge: (i) carry out the processing in a lawful and correct manner, exclusively for the purpose of providing the services covered by the contractual relationship between the Parties; (ii) process personal data solely for purposes inherent to the tasks assigned to them; (iii) do not communicate or disseminate personal data without the prior authorization of the Data Controller; (iv) verify, in case of even temporary interruption of work, that the processed personal data are not accessible to unauthorized third parties; (v) guard and keep authentication credentials strictly confidential; (vi) comply with the security measures required by the Data Controller and/or the Data Controller;

(c) ensure adequate and proven training for persons authorized to process, pursuant to Article 29 of the GDPR;

(d) take, pursuant to Article 32 of the GDPR, all appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art and the costs of implementation, as well as the nature, object, context and purposes of the processing, as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, so as to minimize the risks of destruction or loss, including accidental loss of the data themselves, of unauthorized access or processing that is not permitted or not in accordance with the purposes of collection

e) to inform the Data Controller, in accordance with Article 28 GDPR, if it is necessary to use another Data Processor;

f) assist the Controller in complying with the legal obligations under Articles 32 (Security of Processing), 33 (Notification of a Personal Data Breach to the Supervisory Authority), 34 (Notification of a Personal Data Breach to the Data Subject), 35 (Data Protection Impact Assessment), 36 (Prior Consultation), taking into account the nature of the processing and the information available to the Controller.

g) provide for the updating, modification, rectification of personal data if this is necessary in relation to the purposes of the processing, and delete or return promptly, upon the request of the Controller, all personal data and existing copies of which the Responsible is in possession without being able to retain any copies, unless expressly agreed otherwise or provided for by law. In any case, delete and/or destroy, as required by law (such as "wiping" for digital data), personal data when the purposes for which the data were collected and processed have been achieved in the absence of a legal obligation or the need for further retention;

h) allow the Controller to exercise the power of control under Article 28 GDPR: in this context, make available to the Controller all information necessary to demonstrate compliance with the obligations of this Addendum and to demonstrate compliance with legal obligations and allow verification activities (Audit), carried out by the Controller or by third parties commissioned by the Controller, in order to ascertain the observation of these data processing methods and compliance with legal requirements. The Data Controller shall have the right to verify, with at least 20 (twenty) working days' notice, also at the Data Controller's premises, the compliance of the procedures adopted by the latter with what is indicated in this Addendum or required by law;

i) undertake to comply with the General Provision of the Guarantor for the Protection of Personal Data of November 27, 2008 "Measures and expedients

prescribed for the holders of data processing carried out with electronic instruments in relation to the attributions of the functions of system administrator" as amended by the Order of the Guarantor of June 25, 2009 "Amendments to the order of November 27, 2008 on prescriptions to the holders of processing carried out with electronic tools with regard to the attributions of system administrator and extension of the time limits for their fulfillment," as may be amended or replaced by the same Guarantor, and to any other relevant measure of the Authority;

j) to cooperate for the purposes of the exact application of the law, including through periodic meetings and to act within the scope and limits of their duties, autonomously, but always in accordance with the directives established by the Controller.

5. SUPERVISION. The Data Controller may supervise the punctual compliance with the instructions given herein to the Data Processor and will verify the continuation of the requirements of experience, capacity and reliability that influenced the designation of the Data Processor.

6. VIOLATION. The Processor is hereby made aware that if he/she violates the provisions of the law by independently determining the purposes and means of the Processing, or disregarding the instructions received from the Controller, he/she will be considered the Controller of the Processing in question;

7. ASSISTANCE TO THE CONTROLLER IN CASE OF A BREACH. In the event of a personal data breach, the Provider agrees to inform the Controller without undue delay from the time it has knowledge of the breach. The Supplier shall assist the Holder by initiating a preliminary analysis aimed at collecting data concerning the anomaly and compiling an event sheet, containing all information collected and at that time available, such as, but not limited to:
- Date of event, also the presumed date of occurrence of the violation (in which case it should be specified)
- Date and time when knowledge of the violation was obtained;
- Reporting source;
- Type of violation and information involved;
- Description of abnormal event;
- Number of data subjects involved;
- Numerousness of personal information alleged to have been breached;
- Indication of the date, including alleged date, of the breach and when it became Knowledge;
- Indication of the place where the data breach occurred, also specifying whether it occurred
Occurred as a result of loss of devices or portable media;
- Concise description of the data processing or storage systems involved, with

indication of their location.

8. CONFIDENTIALITY. The Processor agrees to keep strictly confidential and confidential and to use only for the performance of the obligations under the contract, any information relating to the other Party and/or those involved in the processing of personal data and/or products, services, organization, business or technical strategy received from the other Party or of which come to their knowledge during the execution of the contract related to the Service (hereinafter referred to as "Confidential Information"). The Responsible Party undertakes not to use the Confidential Information outside the purposes envisaged by this agreement, nor to disclose it to parties not envisaged by this agreement, without the written approval of the Owner. The Manager shall take all necessary measures not to disclose or make available in any way the Confidential Information of the Owner and/or interested parties to third parties, and shall in any case be held directly liable to the Owner for any violation by its employees and/or subcontractors of the confidentiality obligations set forth in this article. The provisions of this Article shall not apply or shall cease to apply to those individual pieces of information that the Controller can prove: (i) have already become public knowledge for reasons other than the breach by the Controller itself; (ii) were already known prior to having been received by the Controller; (iii) were disclosed or disclosed in compliance with a lawful order of any authority or by virtue of a legal obligation. Disclosed Confidential Information shall remain the property of the Data Controller. Upon written request by the Owner itself such information shall be returned or destroyed by the Responsible Party.

9. AMENDMENTS AND ADDITIONS. The Parties shall have the right to make such amendments and adjustments to this Agreement as may be necessary at any time, including to comply with any regulatory updates. Notice of any request for amendment will be given to the Manager by registered letter with return receipt or certified e-mail. Following the aforementioned change request, the Manager will have 60 days to withdraw from the agreement. After this period, the changes will be deemed accepted by the Processor. For anything not expressly provided for in this agreement, please refer to the general provisions in force regarding the protection of personal data.

10. APPLICABLE LAWS. In the event of any dispute concerning the validity, interpretation, performance and termination of this Addendum, the Parties agree to seek a fair and amicable settlement among themselves. Should the dispute not be settled amicably, it shall be deemed to fall under the exclusive jurisdiction of the Judicial Authority of the Court of Rome. For the resolution of any dispute concerning the validity, interpretation, execution and termination of this agreement the Italian Law will be applied.

It is understood that this appointment does not imply any right of the Supplier to any specific compensation and/or indemnity and/or reimbursement arising from this appointment, beyond what is already provided for in the terms and conditions.