DATA PROCESSING ADDENDUM

PURSUANT TO ART. 28 REGULATION (EU) 2016/679

This Data Processing Addendum (the "DPA") supplements the Master Service Agreement (as updated from time to time) and all other agreements between Client, as data controller ("**Data Controller**" or "**Controller**") represented by its Legal Representative *pro tempore*, and Trustfull governing Client's use of Trustfull's services.

The Client agrees to be bound by this DPA and comply with the terms and conditions set out herein by (a) indicating its acceptance on Trustfull's website or (b) executing a copy of this DPA and returning it to Trustfull.

THE CLIENT HEREBY APPOINTS

Fido SpA with registered office in Via Meravigli 16, 20123, Milan, P.IVA IT09514530964, as data processor ("**Data Processor**" or "**Processor**") represented by its Legal Representative *pro tempore* pursuant to art. 28 of Regulation (EU) 679/2016 of the European Parliament and Council of 27 April 2016 applicable from 25 May 2018 ("**GDPR**").

Whereas:

- Data Controller decided to adopt a risk analysis and scoring system that uses artificial intelligence, in order to implement its risk assessment capacity, through the use of soft data.
- Trustfull is a digital credit & risk scoring company that has created a European platform that uses artificial intelligence to verify the creditworthiness of the new online consumers using a digital footprinting system.
- The Data Processor is going to provide to the Data Controller services concerning risk assessment and scoring of the users who visit the Data Controller website, according to a master service agreement concluded between the parties ("**Agreement**").
- The details of the service and each single processing activity are described in clause 2 of the service Agreement signed by the parties.
- The performance of such services involves the processing of personal data on behalf of the Data Controller.

1. PROCESSING CARRIED OUT BY THE PROCESSOR AND INSTRUCTIONS

1.1. The Processor is authorised by the Controller to process the Personal Data in order to provide the services covered by the service Agreement, within the limits of the Agreement provisions.

1.2. As specified below, Personal Data is processed by the Processor on behalf of the Controller for processing activities related to the execution of activities carried out for the e-commerce activities.

2. DEFINITIONS

2.1. **Processing:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.2. **Personal Data:** any information relating to an identified or identifiable natural person ('**Data Subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3. **Special Categories of Personal Data:** Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as 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.

2.4. **Judicial Data:** Personal Data relating to criminal convictions and offences or related security measures; this type of data may only be processed within the limits and in the cases explicitly provided for by art. 10 GDPR.

2.5. **Data Protection Officer (DPO):** the subjects designated by the Controller and/or Processor as being in charge of data protection.

3. DUTIES OF THE PROCESSOR

3.1. The Processor shall process the Personal Data ("**Data**") on behalf of the Controller as established by the applicable law and, in particular, by the GDPR.

3.2. The Processor acts according to the instructions of the Controller, as below.
3.3. Duties of the Processor:
- 3.3.1. to process the Data exclusively for the purposes of the processing carried out on behalf of the Controller;
- 3.3.2. to process the data according to the written instructions of the Controller, as set out in the Agreement. Furthermore, if the Processor has to transfer data to a third (non-EU) country or to a third party organisation, in accordance with European Union law or a Member State law to which the Processor is subject, the Processor shall inform the Controller of this legal requirement before processing, unless that law prohibits such information for public interest reasons;
- 3.3.3. to guarantee the confidentiality of the Data processed under the Agreement;
- 3.3.4. to inform the Controller without undue delay of any substantial change that has affected the security measures regarding the processing;
- 3.3.5. to guarantee that the personnel authorised to process the Data under the Agreement:
  - 3.3.5.1. respects confidentiality or is subject to an adequate obligation of confidentiality;
  - 3.3.5.2. receives the necessary training on data protection;
  - 3.3.5.3. does not process data except on indication and according to the instructions of the Processor;
- 3.3.6. to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR and ensures the protection of data subject rights;
- 3.3.7. to immediately inform the Controller of any request and/or inspection by the Data Protection Authority regarding the processing of Data carried out pursuant to the Agreement. In the case of controls at the offices of the Processor, the latter agrees that a person specifically appointed for this purpose by the Controller shall be present at the time of the check by the proceeding Data Protection Authority ("**DPA**");
- 3.3.8. to respect all the obligations established by article 6 below in the event of a data breach;
- 3.3.9. to collaborate according to the instructions of the Controller in the case of a citation, injunction, formal notification or any other decision from the DPA or any other competent Authority or assist the Controller in preparing the responses to the said Authorities;
- 3.3.10. except as indicated below, not to transfer or communicate all or part of the data processed to another person or body, even free of charge.

4. USE OF SUB PROCESSORS

4.1. The Data Processor is entitled to delegate to third parties the performance of processing activities related to the performance of services under the Agreement. In any case, the Data Processor is responsible for ensuring that its (Sub) Data Processor provides sufficient guarantees on the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the Regulation. If the (SUB) Data Processor fails to comply with its obligations with respect to data protection, the Data Processor shall remain fully responsible to the Controller for the performance of its (Sub) Data Processor's obligations.

5. DATA SUBJECT RIGHTS

5.1. The Processor shall assist the Controller to carry out its obligations to handle requests from Data Subjects who intend to exercise their rights such as: right of access, rectification, erasure, and opposition, right to limit processing, right to data portability, right not to be subject to automated individual decisions (including profiling).
5.2. When the Data Subjects submit their requests to the Processor, the latter shall notify the Controller within five (5) days.
5.3. In all cases, the Processor undertakes to send all the necessary elements, if available, to the Controller within fifteen (15) working days of the request.

6. NOTIFICATION OF PERSONAL DATA BREACH

6.1. The Processor shall notify the Controller of any Data breach within forty-eight (48) hours from the time it becomes known by sending an e-mail to the address associated with the Client's administrative user in Trustfull Platform
6.2. The notification is accompanied by the relative documentation so that the Controller, if necessary, can notify the relevant Data Protection Authority (DPA) of the breach.
6.3. The Processor shall not report the breach to the Data Protection Authority or to the Data Subjects without first having obtained the written consent of the Controller.
6.4. The Data breach notification sent by the Processor to the Controller shall include at least the following:
- 6.4.1. the description of the nature of the Data breach, if possible, including the categories of the approximate number of Data Subjects involved in the breach and the categories and approximate amount of Personal Data involved;
- 6.4.2. the names and contact details of the Data Subjects involved in the Data breach;
- 6.4.3. the name and contact details of the Data Protection Officer or other contact point from which additional information can be obtained;
- 6.4.4. the description of the possible consequences of the Personal Data breach;

6.4.5. the description of the measures adopted or that the Processor proposes to resolve the Personal Data breach, including, where applicable, measures to reduce all negative consequences of the breach.

6.5. If it is not possible to provide all this information immediately, the Processor shall ensure it will be sent to the Controller as soon as it becomes available.

7. OTHER INSTRUCTIONS

7.1. If necessary, the Processor assists the Controller to conduct the impact assessments related to the protection of personal data ("**DPIA**") pursuant to Article 35 of the GDPR.

7.2. If the Controller considers that the processing represents a high risk for the rights of the Data Subjects as a consequence of the DPIA, the Processor shall support the Controller in first consulting the DPA.

7.3. If, at the end of the consultation, the DPA considers that the processing must be modified, this activity will be carried out by the Processor at its own expense.

8. SECURITY MEASURES

8.1. The Data Processor declares and guarantees it has adopted and, in any case, undertakes to adopt all the security measures necessary to protect the data processed on behalf of the Controller and its information systems from intrusion or unauthorised access, from acts of destruction or alteration, from contamination by malicious software or any other event that threatens the integrity, availability or confidentiality of the data, or that could cause anomalies that could prejudice data security, by 25 May 2018.

8.2. The Processor undertakes to implement the following security measures:

8.2.1. adoption of resources to ensure the confidentiality, integrity, availability and constant resilience of processing systems and services;

8.2.2. use of resources to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

8.2.3. adoption of a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.3. Furthermore, the Processor undertakes to do everything in its power to promptly resolve security incidents that may occur. The Processor undertakes to inform the Controller within forty-eight (48) hours of the discovery of the event, to the email address associated with the Client's administrative user in Trustfull Platform

8.4. Finally, in the event of a Personal Data breach, the Processor undertakes to inform the Controller within forty-eight (48) hours.

9. FUTURE OF DATA

9.1. At the end of the services provision relating to the processing of data, the Processor, subject to Agreement with the Controller and where applicable law does not impose otherwise, undertakes to:

9.1.1. destroy all Personal Data or

9.1.2. return all Personal Data to the Controller or

9.1.3. return all Personal Data to the Processor indicated by the Controller.

9.2. At the time of the eventual return of the data, all existing copies on the information systems of the Processor shall be destroyed. After destruction, the Processor shall send the Controller a declaration stating that all the data present on all fixed and mobile devices have been destroyed. This is without prejudice to the right of the Controller to verify this circumstance by accessing the site and systems of the Processor.

10. DATA PROTECTION OFFICER (DPO)

10.1. If a DPO is appointed the Processor will send to the Controller the details (first name, last name, e-mail address, telephone number and address) of the designated Data Protection Officer, pursuant to Article 37 of the Regulation.

11. RECORD OF PROCESSING ACTIVITIES

11.1. The Processor undertakes to keep a record of all the processing carried out on behalf of the Controller ("**Record**").

11.2. The Record shall contain at least the following:

11.2.1. the name and contact details of the Controller on whose behalf it is acting, any sub-processors and people in charge of the processing and, where applicable, its Data Protection Officer;

11.2.2. the categories of processing carried out on behalf of the Controller;

11.2.3. where applicable, transfers of personal data to a third country (Extra EU) or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

11.2.4. as far as possible, a general description of the organisational and technical security measures, including, inter alia, for example:

11.2.4.1. the pseudonymisation and encryption of personal data;
11.2.4.2. the resources to ensure the confidentiality, integrity, availability and constant resilience of processing systems and services;
11.2.4.3. the resources to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
11.2.4.4. the process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

12. AUDIT

12.1. The Processor undertakes to guarantee complete and immediate access to the Controller to its activities, site and documentation relating to the processing carried out on behalf of the Controller, in order to carry out checks and inspections, as well as to send requests for data and news directly to the Processor.
12.2. The Processor provides the Controller with the documentation necessary to demonstrate compliance with all obligations set by the Controller and to allow audits and inspections to be carried out by the Controller or by its representatives.

13. DAMAGES AND INDEMNITY

13.1. Notwithstanding any clauses limiting liability in the Agreement, the Processor shall guarantee and indemnify the Controller for damages, including operational and reputational damages and penalties claimed by Controller due to the non-execution by the Processor of the obligations incumbent upon it in relation to the provisions of the applicable legislation on the protection and processing of personal data.

14. ACCEPTANCE OF APPOINTMENT

14.1. By entering into this Data Processing Addendum, pursuant to art. 28 GDPR, the Data Processor accepts its appointment, in relation to Personal Data whose knowledge is essential for the fulfilment of the obligations under the Agreement. The Data Processor is aware of the obligations provided for in the Regulations and shall comply with the provisions and obligations contained in this deed for the performance of the activities assigned to him/her.
14.2. This appointment will last until the end, for whatever reason, of the Agreement entered into between the Parties.

Signatures

Fido SpA	Client
	Client Legal Name:
Name:	Name:
Date:	Date: