Information about this Data Processing Addendum

This Data Processing Addendum (DPA) is addressing Article 28 GDPR.

Please download this Data Processing Addendum (DPA) if you need it as part of your GDPR compliance efforts. The DPA is pre-signed and can be signed by you as the Client party. If you have any questions or comments, we are happy to help: support@judge.me.

You can send your signed version directly to: pj@judge.me

PJC

JUDGE.ME DATA PROCESSING ADDENDUM

This Data Protection Addendum ("DPA") forms part of the Terms of Service between:
(i) Judge.me LLC ("Provider"); and

(ii) _____ ("Client") acting on its own behalf to reflect the parties' agreement with regard to the Processing of Personal Data.

In the course of providing the Services to the Client pursuant to the Agreement, Judge.me may process Personal Data on behalf of the Client and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

PJC

Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

"**Applicable Laws**" means (a) European Union or Member State laws with respect to any Client Personal Data subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Client Personal Data subject to any other Data Protection Laws;

"**Client Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a the Client pursuant to or in connection with the Terms of Service;

"**Contracted Processor**" means Provider or a Sub-processor;

"**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

"**EEA**" means the European Economic Area;

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

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

"**Restricted Transfer**" means:

- a transfer of Client Personal Data to a Contracted Processor; or
- an onward transfer of Client Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses;

"**Services**" means the services and other activities to be supplied to or carried out by or on behalf of the Provider for the Client pursuant to the Terms of Service;

"**Standard Contractual Clauses**" means the agreement executed by and between Client and Judge.me LLC pursuant to the European Commission's decision (C(2010)593) on Standard Contractual Clauses for the transfer of personal data to

PJC

processors established in third countries which do not ensure an adequate level of data protection;

"**Sub-processor**" means any person (including any third party and any Provider Affiliate, but excluding an employee of the Client or any of its sub-contractors) appointed by or on behalf of the Client to Process Personal Data on behalf of the Client in connection with the Terms of Service.

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

Authority

Legal Authority. Client signatory represents to Provider that he or she has the legal authority to bind Client and is lawfully able to enter into contracts (e.g., is not a minor).

Termination. This Addendum will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder or by the Provider's Terms and Conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this Addendum or (iii) as agreed by the parties in writing.

Processing of Personal Data

The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Data Controller, Provider is a Data Processor and that Provider will engage Sub-processors pursuant to the requirements set forth in Section "Sub-processors" below.

1.1 Provider shall:

1.1.1 comply with all applicable Data Protection Laws in the Processing of Client Personal Data; and

1.1.2 not Process Client Personal Data other than on the Client's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Provider shall to the

extent permitted by Applicable Laws inform the Client of that legal requirement before the relevant Processing of that Personal Data.

1.2 Client Shall

1.2.1 instructs Provider and authorises Provider to instruct each Sub-processor to:

1.2.1.1 Process Client Personal Data; and

1.2.1.2 in particular, transfer Client Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Terms of Service; and

1.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 1.2.1.

1.2.3 In addition, Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data. Personal Data provided by the Client shall not contain information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric, data concerning health or data concerning an individual's sex life or sexual orientation ("Special Categories of Data").

1.3 **Provider's Processing of Personal Data.**

1.3.1 Provider shall only Process Client Personal Data for the purpose of the provision of the Services under the Agreement and in accordance with Client's documented instructions which are consistent with the terms of the Agreement, unless Processing is required by Data Protection Laws to which Provider (or the applicable sub-processor) is subject, in which case Provider shall to the extent permitted by the Data Protection Laws inform Client of that legal requirement before the relevant Processing of that Client Personal Data.

1.3.2 This Addendum and the Agreement are Client's complete and final instructions to Provider for the Processing of Client Personal Data. Any additional or alternate instructions must be agreed upon separately.

1.3.3 The following are deemed instructions of the Client to Provider: The processing of Client Personal Data (i) in accordance with the Agreement and this Addendum, including without limitation with the transfer of Client Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Agreement.

1.4 Exhibit A to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Client Personal Data as required by article 28(3) of the

GDPR and, possibly, equivalent requirements of other Data Protection Laws. Client may make reasonable amendments to Exhibit A by written notice to Provider from time to time as Client reasonably considers necessary to meet those requirements. Nothing in Exhibit A, including as amended pursuant to this section 1.3, confers any right or imposes any obligation on any party to this Addendum.

Provider Personnel

Provider shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Client Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Client Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Sub-processors

Appointment of Sub-processors. For the purpose of the appointment of Sub-processors, Client acknowledges and agrees that Provider may engage third-party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Client Personal Data.

List of Current Sub-processors and Notification of New Sub- processors. When requested by the Client, the Provider shall make available to Client an up-to-date list of all Sub-processors used for the processing of Client Personal Data.

Objection Right for New Sub-processors. Provider shall give Client prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within 14 days of receipt of that notice, Client notifies Provider in writing of any objections (on reasonable grounds) to the proposed appointment, then (i) Provider shall work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and (ii) where such a change cannot be made within 14 days from Provider's receipt of Client's notice, notwithstanding anything in the Agreement, Client may by written notice to Provider with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

Sub-processing Agreement; Liability. Provider has or shall enter into a written agreement with each Sub-processor (the “Sub-processing Agreement”) containing data protection obligations not less protective than those in the Agreement and/or this Addendum with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services

PJC

provided by such Sub-processor. Provider shall be liable for the acts and omissions of its Sub-processors to the same extent Provider would be liable if performing the services of each Sub-processor directly under the terms of this Addendum.

Copies of Sub-Processor Agreements. Provider shall provide to Client for review copies of the Sub-processor agreements as Client may reasonably request from time to time. The parties agree that all commercial information may be removed by the Provider beforehand.

Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Provider shall in relation to the Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

In assessing the appropriate level of security, Provider shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

Data Subject Rights

Taking into account the nature of the Processing, Provider shall assist Client by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

Provider shall:

- promptly notify Client if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Client Personal Data; and
- ensure that the Contracted Processor does not respond to that request except on the documented instructions of Client or as required by Applicable Laws to which the Contracted Processor is subject, in which case Provider shall to the extent permitted by Applicable Laws inform Client of that legal requirement before the Contracted Processor responds to the request.

Personal Data Breach

Personal Data Breach notification. Provider shall notify Client without undue delay upon Provider or any Sub-processor becoming aware of a Personal Data Breach affecting Client

Personal Data, providing Client with sufficient information to allow Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

Personal Data Breach mitigation. Provider shall cooperate with Client and take such reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

Data Protection Impact Assessment and Prior Consultation

Provider shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

Return or Destruction of Personal Data

Return or Deletion. Subject to the provisions of the Section below, at Client's election, made by written notice to Provider following 30 days of the date of cessation of any Services involving the Processing of Client Personal Data (the "Cessation Date"), Provider shall, and shall procure that all Sub-processors: (a) return a complete copy of all Client Personal Data to Client in such format and manner requested by Client and reasonably acceptable to Provider; and (b) delete and procure the deletion of all other copies of Client Personal Data Processed by Provider or any Sub-processor. Provider shall comply with any such written request within 30 days of the Cessation Date.

Retention of Copies. Provider and each Sub-processor may retain Client Personal Data to the extent required by applicable European Union law or the law of an EU Member State and only to the extent and for such period as required by such laws and always provided that Provider shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in such law requiring its storage and for no other purpose.

Notification. Provider shall provide written certification to Client that it and each Sub-processor has fully complied with this section within 14 days of the Cessation Date.

PJC

Audit rights

1.1 Subject to sections 1.2 to 1.4, Provider shall make available to Client on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Client or an auditor mandated in relation to the Processing of the Client Personal Data by the Contracted Processors.

1.2 Information and audit rights of the Client only arise under this section to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

1.3 Client undertaking an audit shall give Provider reasonable notice of any audit or inspection to be conducted under section 1.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

1.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

1.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Client undertaking an audit has given notice to Provider that this is the case before attendance outside those hours begins; or

1.3.3 for the purposes of more than 1 audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

1.3.3.1 Client undertaking an audit reasonably considers necessary because of genuine concerns as to Provider's compliance with this Addendum; or

1.3.3.2 Client is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Client undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Provider of the audit or inspection.

PJC

Restricted Transfers

1.1 Subject to section 1.3, the Client (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses (Article 26(2) of Directive 95/46/EC) in respect of any Restricted Transfer from the Client to that Contracted Processor.

1.2 The Standard Contractual Clauses shall come into effect under section 1.1 on the later of:

1.2.1 the data exporter becoming a party to them;

1.2.2 the data importer becoming a party to them; and

1.2.3 commencement of the relevant Restricted Transfer.

1.3 Section 1.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

General Terms

Governing law and jurisdiction. Without prejudice to clauses on Mediation and Jurisdiction and Governing Law of the Standard Contractual Clauses:

- the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
- this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Terms of Service.

Order of precedence. Nothing in this Addendum reduces Provider's obligations under the Terms of Service in relation to the protection of Personal Data or permits Provider to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Terms of Service. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

Subject to the above, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Terms of Service and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

PJC

Severance

Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (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.

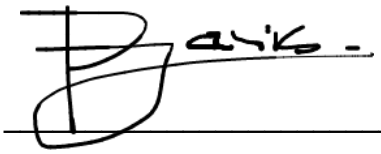
Indemnification; Limitation of Liability

If one party is held liable for a violation of this Addendum or, if applicable, any provision of the Standard Contractual Clauses, committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred in accordance with the provisions of the "Indemnification" Section of the Agreement. Each party's liability, taken together in the aggregate, arising out of or related to this Addendum and/or the Standard Contractual Clauses, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement. For the avoidance of doubt, Provider's total liability for all claims from the Client or any third party arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and this Addendum.

EXECUTED by and on behalf of:

Provider Name: Peter-Jan Celis: Founder & CEO

Date: 05 / 24 / 2018



_____

EXECUTED by and on behalf of:

Client Name:

Date:

_____

EXHIBIT A: DETAILS OF PROCESSING

This Exhibit A includes details of the Processing of Client Personal Data as required by Article 28(3) GDPR.

1. PROCESSING BY THE PROVIDER

1.1 SCOPE

The scope of processing data subjects' personal data is information related to the purchase and review. Additionally we process personal data about the client to enable certain functions or support.

1.2 NATURE

We process data subjects' personal data that is provided by your platform, website or you directly. We use sub-processors to facilitate our services. We are not processing special categories of personal data.

1.3 PURPOSE

The purpose of processing of the data subjects' personal data is to facilitate the provision of provider's services.

1.4 DURATION

The duration of the processing of the client's personal data are set out in the Terms of Service and this Addendum.

2. CATEGORIES OF DATA SUBJECT

Personal data of the following categories of data subjects is processed:

- Client's customers and other client's end-users (website visitors)
- Client and Client's representatives

3. TYPES OF PERSONAL DATA

The following types of personal data is processed:

- Client's customers
    - Name, Email
    - Review content
    - Order, fulfillment information
    - Email event information
    - IP for location information
- Client and Client's representatives

PJC

- Name, email and phone number (for providing customer support)
- Admin email address (to send notifications)
- Email info, that is sender name, email address (to send email on behalf of you)
- Facebook user access token (for social push)

PJC

EXHIBIT B: SECURITY MEASURES

1. **Personnel.** Data Importer's personnel will not process customer data without authorization. Personnel are obligated to maintain the confidentiality of any customer data and this obligation continues even after their engagement ends.
2. **Data Privacy Contact**

   Judge.me LLC
   Attn: Peter-Jan Celis
   PO Box 7403
   Jackson, WY 83002 (U.S.A.)

3. **Technical and Organization Measures.** The Data Importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

   3.1. **Organization of Information Security.**

   A. Security Roles and Responsibilities. The Data Importer has appointed Linh Dam as the security officer responsible for coordinating and monitoring the security rules and procedures.

   B. Duty of Confidentiality. The Data Importer's personnel with access to customer data are subject to confidentiality obligations.

   3.2. **Risk Management.** The Data Importer conducts regular testing and monitoring of the effectiveness of its safeguards, controls, systems. The Data Importer implements measures, as needed, to address vulnerabilities discovered in a timely manner.

   3.3. **Storage.** The Data Importer's database servers are hosted in a data center operated by a third party vendor, that has been qualified per the Data Importer's vendor management procedure. The Data Importer maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to customer data.

   3.4. **Asset Management.** The Data Importer maintains an inventory of all media on which customer data is stored. Access to the inventories of such media is restricted to authorized personnel.

   3.5. **Software Development and Acquisition:** For the software developed by Data Importer, Data Importer follows secure coding standards and procedures.

   3.6. **Third Party Provider Management:** In selecting third party providers who may gain access to, store, transmit or use customer data, Data Importer conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

   3.7. **Human Resources Security.** The Data Importer informs its personnel about relevant security procedures and their respective roles, as well as of possible

PJC

consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

3.8. **Data Recovery Procedures.**

i. On an ongoing basis, the Data Importer maintains multiple copies of customer data from which it can be recovered.

ii. The Data Importer stores copies of customer data and a data recovery procedures in a different place from where the primary computer equipment processing the customer data is located.

iii. The Data Importer has procedures in place governing access to copies of customer data.

iv. The Data Importer has anti-malware controls to help avoid malicious software gaining unauthorized access to customer data.

3.9. **Information Security Incident Management.**

a. Record of Breaches. The Data Importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

b. Record of Disclosure. The Data Importer tracks disclosures of customer data, including what data has been disclosed, to whom, and at what time.

PJC