DATA PROTECTION ADDENDUM

This Data Protection Addendum ("DPA") is made as of _____ (the "Effective Date") by _____with its principal place of business at _____ (collectively, "Customer", "you," "Data Exporter", "Controller", or "Subprocessor") and ProsperWorks, Inc. (collectively, "ProsperWorks," "we," "our," "Data Importer" or "Processor"), with its principal place of business at 301 Howard Street #600, San Francisco, California, 94105. This DPA supplements any existing and currently valid ProsperWorks Subscription Agreement, ProsperWorks Terms of Service, or other agreement previously made between ProsperWorks and you pursuant to which you obtain access to the Services (collectively, "Agreement").

The terms of this DPA will prevail over any conflicting terms in the Agreement. All capitalized terms that are not expressly defined in the DPA will have the meanings given to them in the Agreement.

In addition to Part A (General Information Security Terms), Part B (Personal Information that Originated in the European Economic Area or Switzerland) of this DPA will apply to the extent ProsperWorks Processes Personal Information that originated in the EU.

PART A

1. Definitions; Interpretation.

(a) "**Applicable Laws**" means all privacy, data security, and data protection laws, directives, regulations, and rules in any jurisdiction applicable to ProsperWorks and the Services under the Agreement, including, where applicable, EU Data Protection Law.

(b) **"EU"** means European Union, European Economic Area, United Kingdom, or Switzerland

(c) "**EU Data Protection Law**" means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and applicable successor data protection regulation(s) ("**The Directive**"), and on and after May 25, 2018, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "**GDPR**").

(d) "**EU-US Privacy Shield**" means the agreement between the United States Department of Commerce and the European Union that regulates transferring Personal Data from the European Union and European Economic Area ("EU") to the United States ("US"), and which replaces the US-EU Safe Harbor Privacy Framework.

(e) **"Swiss-US Privacy Shield"** means the agreement between the United States Department of Commerce and Switzerland that regulates transferring Personal Data from Switzerland to the United States, and which replaces the US-Swiss Safe Harbor Privacy Framework.

(f) "**includes**" or "**including**" means, "including but not limited to".

(g) "**Personal Information**" means (i) any information about an identifiable individual; or (ii) information that is not specifically about an identifiable individual but, when combined with other information, may identify an individual. Personal Information includes names, email addresses, postal addresses, telephone numbers, government identification numbers, financial account numbers, payment card information, credit report information, biometric information, IP addresses, network and hardware identifiers, and geolocation information. In this Agreement, "Personal Information" has the same meaning as "**personal data**" under EU Data Protection Law.

(h) **"Process" or "Processing**" means to create, collect, receive, acquire, record, consult, alter, use, process, store, retrieve, maintain, disclose, or dispose of

(i) "**Protected Information**" means Personal Information that we or a Third Party Provider may Process in performing Services. Protected Information does not include the parties' business contact information (specifically, business addresses, phone numbers, and email addresses) including the party's contact persons' names used solely to facilitate the parties' communications for administration of the Agreement.

(j) "**reasonable**" means reasonable and appropriate to (i) the size, scope, and complexity of ProsperWorks' business; (ii) the nature of the Personal Information being Processed; and (iii) the need for privacy, confidentiality, and security of the Protected Information.

(k) "**Safeguards**" has the meaning set forth in Section 4 (Safeguards).

(l) "**Security Incident**" means an actual or reasonably likely loss of or unauthorized Processing to Protected Information in ProsperWorks' custody or control.

(m) "**Services**" means any goods or services that ProsperWorks provides to you under the Agreement.

(n) "**Third Party Provider**" means any contractor or other third party that ProsperWorks authorizes to act on its behalf in connection with performing Services.

2. Compliance with Laws; Use Limitation; Privacy Notice.

(a) Compliance with Applicable Laws. We represent and warrant that when we Process Protected Information under the Agreement, we will at all times comply with all Applicable Laws, including any requirements that apply to cross--border transfers of Personal Information.

(b) Use Limitation. We will Process Protected Information solely to exercise our rights and to fulfill our obligations under the Agreement. We will not Process the Protected Information for any other purpose.

3. Third Party Providers. We are responsible for our Third Party Providers' acts and omissions. We will contractually require each Third Party Provider that has access to Protected Information to protect the privacy, confidentiality, and security of Protected Information using at least the same level of protection and confidentiality obligations that apply to us under this DPA. We will provide you with names and addresses of Third Party Providers if required by Applicable Law.

4. Safeguards. At all times that we Process Protected Information, we will maintain reasonable administrative, technical and physical controls designed to ensure the privacy, security, and confidentiality of the Protected Information ("**Safeguards**"), that comply with this DPA, and Applicable Laws, including:

(a) Physical Access. We will maintain physical access controls designed to secure relevant facilities, infrastructure, data centers, hard copy files, servers, backup systems, and ProsperWorks-owned equipment (including mobile devices) used to access Protected Information, including controls to prevent, detect, and respond to attacks, intrusions, or other system failures;

(b) User Authentication. We will maintain user authentication and access controls within operating systems, applications, and equipment;

(c) Personnel Security. We will maintain personnel security policies and practices restricting access to Protected Information, including written confidentiality agreements and background checks consistent with Applicable Law for all personnel with access to Protected Information or who maintain, implement, or administer our information security program and Safeguards;

(d) Logging and Monitoring. We will log and monitor access to Protected Information on networks, systems, and devices operated by us.;

(e) Malware Controls. We will maintain reasonable and up-to-date controls to protect all networks, systems, and devices that access Protected Information from malware and unauthorized software; and

(f) Security Patches. We will maintain controls and processes designed to ensure that networks, systems, and devices (including operating systems and applications) that access Protected Information are up-to-date, including prompt implementation of identified high severity security patches when issued.

5. Access Controls. We will:

(a) Maintain reasonable controls to ensure that only personnel who have a legitimate need to Process Protected Information under the Agreement will have such Processing ability; and

(b) Promptly terminate personnel access to Protected Information when such access is no longer required for performance under the Agreement.

6. Training and Supervision. We will provide reasonable ongoing privacy and information protection training and supervision for all our personnel who access Protected Information.

7. Security Incident Response.

(a) Security Incident Response Program. We will maintain a reasonable incident response program to respond to Security Incidents.

(b) Notice. If a Security Incident occurs, we will promptly, but in no event less than 72 hours following such Security Incident, send an email to your administrative account contact and provide a summary description of the details known about the Security Incident.

(c) Investigation; Remediation. If a Security Incident has occurred, we will promptly (a) investigate Security Incident; (b) remediate the root cause of the Security Incident and provide assurances that the remediation meets this DPA's requirements; and (c) identify relevant contact people who will be reasonably available until the Security Incident has been resolved. The obligations herein shall not apply to incidents that are caused by you or your users of the Services.

(d) No Unauthorized Statements. Except as required by law, we will not make any statement concerning the Security Incident that references you either directly or indirectly unless you provide your written authorization.

8. Legal Process. If we become legally compelled by a court or other government authority to disclose Protected Information, then to the extent permitted by law, we will promptly provide you with sufficient notice of all available details of the legal requirement and reasonably cooperate with your efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action, as we may deem appropriate.

9. Vulnerability Testing.

(a) We will periodically have a third party perform manual and automated vulnerability testing on our networks, systems, software and devices used to access Protected Information.

(b) Upon written request, we will provide you with the summarized results of the vulnerability testing. You will treat these results as ProsperWorks' confidential information.

10. Retention and Destruction of Protected Information.

(a) Retention. We will store and retain any Protected Information as necessary to perform Services under the Agreement and in accordance with our data retention policies.

(b) Destruction. We will destroy Protected Information within 180 days following expiration or termination of the Agreement. If required by Applicable Law, we may retain a copy of the Protected Information for so long as required. Additionally, we may retain a copy of the Protected Information in our backup and archival systems in accordance with our standard operating procedures, provided that the Protected Information is not used for active processing by the Services, unless we restore such data due to a disaster recovery or similar event which requires restoration of such Protected Information. Upon your written request, we will delete any Protected Information from our back-up and archival systems within 30 days following your request.

11. Survival. Obligations under this DPA will survive expiration or termination of the Agreement and completion of the Services as long as we continue to Process Protected Information.

Part B: Personal Information that Originated in the EU

This Part B of this DPA will apply (along with Part A) to the extent we Process Personal Information that originated in the EU.

1. Definitions. Unless otherwise defined in the DPA, all terms in Part B will have the definitions given to them by EU Data Protection Law.

2. Data Processor Obligations: To the extent we Process Personal Information as a "Data Processor", we will:

(a) Process the Personal Information only for the limited and specified purposes stated in the Agreement and not in a way that is incompatible with such purposes;

(b) Notify you of any individuals' access requests or complaints we receive regarding the Personal Information, and cooperate with and assist you in investigating and responding to individuals exercising their legal rights at your expense;

(c) Comply with your written instructions to access, correct, amend, or delete the Personal Information;

(d) To the extent legally permitted, promptly notify you if we receive a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of access, erasure ("right to be forgotten"), data portability, object to the access, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the access, we will assist you by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of your obligation to respond to a Data Subject Request under EU Data Protection Laws. In addition, to the extent you, in its use of the Services, do not have the ability to address a Data Subject Request, we will upon your request provide commercially reasonable efforts to assist you in responding to such Data Subject Request, to the extent we are legally permitted to do so and the response to such Data Subject Request is required under EU Data Protection Laws. To the extent legally permitted, you will be responsible for any costs arising from our provision of such assistance; and

(e) Stop Processing the Personal Information if at any time it is determined by a valid third party authority that we are not Processing the Personal Information in compliance with the Agreement (and the principles of the EU-US Privacy Shield and Swiss-US Privacy Shield, if applicable).

3. Data Controller Obligations: To the extent you provide us with access to Personal Information, you will:

(a) Provide individuals with a clear and conspicuous privacy notice that (i) accurately describes how we Process the Personal Information; and (ii) complies with Applicable Laws;

(b) Obtain consent from individuals, in compliance with Applicable Laws, and using a clear, conspicuous and readily available mechanism, for our Processing of their Personal Information;

4. EU Data Protection Compliance.

(a) Transfers Under the EU-US Privacy Shield. ProsperWorks, Inc. has certified, and will remain certified, to the EU-US Privacy Shield Framework.

(b) Processing EU-Originated Personal Information from Non-Adequate Countries. We will ensure the lawfulness of cross--border transfers of Personal Information by doing one of the following, at our option: (i) entering into an agreement with you based on the European Commission's or Swiss Federal Data Protection and Information Commissioner's standard contractual clauses; (ii) implementing fully

approved binding corporate rules (BCRs) and taking such steps as are required to ensure that the Personal Information is protected by those BCRs; or (iii) where applicable, certifying compliance to the EU-US Privacy Shield and Swiss-US Privacy Shield and complying with its relevant principles.

IN WITNESS WHEREOF, ProsperWorks and _____ have executed this DPA as of the Effective Date.

PROSPERWORKS, INC.

DocuSigned by:
Mary Grayson Thibaut
F0E...

By: _____
Name: Mary Grayson Thibaut
Title: VP Finance & Operations
Date: 4/26/2018

_____
CUSTOMER

By: _____
Name: _____
Title: _____
Date: _____