PrimePay, LLC

Data Processing Addendum

This Data Processing Addendum (the "**DPA**") is made and entered into as of the Effective Date as set forth in the Quote between PrimePay, LLC, a Delaware limited liability company ("PrimePay") and employer who is subject to Applicable Data Protection Laws (defined below) and signed up for certain PrimePay services subject to the PrimePay Product Terms ("Customer") indicated on the signed order form or quote (the "Quote"). Collectively, the Product Terms and Quote shall be referred to as the Agreement. PrimePay and Customer may individually be referred to as a Party, or collectively, the Parties. The Parties agree as follows:

1. DEFINITIONS

1.1 "**Applicable Data Protection Laws**" means the data protection laws, rules and regulations that are applicable to PrimePay and Customer from the European Union, United Kingdom and Switzerland, including, but not be limited to, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

1.2 "**Customer Personal Data**" means Personal Data that is received by PrimePay pursuant to the Agreement and pertains to Customer's current, former, or potential employees, contractors, or other individuals who are, based on information known to PrimePay, residents of the European Union, United Kingdom, or Switzerland, or whose Personal Data is otherwise protected by Applicable Data Protection Laws.

1.3 "**Data Privacy Framework**" or "**DPF**" means the EU-U.S. Data Privacy Framework, the UK Extension to EU-U.S. DPF, and Swiss-U.S. Data Privacy Framework, developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration.

1.4 "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.5 "**EU**" or "**European Union**" means the European Economic Area, as well as the United Kingdom and Switzerland.

1.6 "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Laws.

1.7 "**Process**", "Processes", "Processing", "Processed" shall have the meanings assigned to them in the Applicable Data Protection Laws.

1.8 "**Security Incident**" means an event in which Customer Personal Data held by PrimePay has been, to the knowledge of PrimePay, accessed, disclosed, acquired or used by any unauthorized person, in violation of Applicable Data Protection Laws.

1.9 "**Sub-Processor**" means PrimePay's contractors, agents, vendors, and third-party service providers, that Process Customer Personal Data.

2. DATA HANDLING AND ACCESS

2.1 General Compliance. Customer hereby authorizes and instructs PrimePay to, and PrimePay will, and will require Sub-Processors to, Process Customer Personal Data in compliance with the Agreement, this

DPA, and all Applicable Data Protection Laws. Customer represents and warrants that it has all authority and consents required by Applicable Data Protection Laws for such Processing of the Customer Personal Data.

2.2 PrimePay and Sub-Processor Compliance. PrimePay agrees to (i) enter into a written agreement with each Sub-Processor regarding such Sub-Processor's Processing of Customer Personal Data that imposes on such Sub-Processors data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Laws, and that, at a minimum, require a level of data protection and security equal to or superior to the level of data protection and security under this DPA; (ii) reasonably enforce compliance with such written agreements; and (iii) remain responsible to Customer for the actions or omissions of PrimePay's Sub-Processors (and their sub-processors if applicable) with respect to the Processing of Customer Personal Data.

2.3 Authorization to Use Sub-Processors. Customer hereby authorizes (i) PrimePay to engage Sub-Processors and (ii) Sub-Processors to engage sub-processors. PrimePay will provide Customer, upon Customer's request, the name, address and role of each Sub-Processor used to Process Customer Personal Data and any other records of Processing of Customer Personal Data that Sub-Processors are required to maintain and provide under Applicable Data Protection Laws. Customer hereby approves of PrimePay's Sub-Processors, each of which may Process Customer Personal Data related to one or more services provided by or on behalf of PrimePay.

2.4 Objection Right for New Sub-Processors. PrimePay will inform Customer of any new Sub-Processor in connection with the provision of the applicable Services. Customer may object to PrimePay's use of a new Sub-Processor by notifying PrimePay promptly in writing within ten (10) business days after receipt of such information. In the event Customer objects to a new Sub-Processor, as permitted in the preceding sentence, PrimePay may address the concerns with respect to the Sub-Processor, or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to Sub-Processor without unreasonably burdening the Customer. If PrimePay does not do so within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the Services which cannot be provided by PrimePay without the use of the objected-to new Sub-Processor by providing written notice to PrimePay.

2.5 Following Instructions. PrimePay will Process Customer Personal Data only in accordance with the written instructions of Customer, which include instructions to Process Customer Personal Data: (i) in accordance with the Agreement and applicable Order Form(s); (ii) as initiated by users in their use of the Services; (iii) to further develop and provide services to PrimePay's customers; (iv) to facilitate the anonymization of Personal Data; and (v) to comply with other documented reasonable instructions provided by Customer (e.g., via email). PrimePay will disclose Customer Personal Data to third parties (including other Customer processors) as instructed by Customer and Customer represents and warrants that there is a legal basis for each such disclosure.

2.6 Details of the Processing. The subject matter of Processing of Personal Data by PrimePay is the performance of the Services pursuant to the Agreement. Customer Personal Data may be transferred on a continuous basis for the term of the Agreement, as provided in the DPA, and as otherwise agreed upon in writing. Personal Data may be transferred through a third party hosted cloud environment or through SFTP or API protocols. All transfers shall be in accordance with the DPA. For more information regarding PrimePay's Processing of Customer Personal Data, please see PrimePay's Privacy Policy, available here.

3. EU LAWS

3.1 Rights of Data Subjects. PrimePay will, to the extent legally permitted, promptly notify Customer if PrimePay receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). To the extent Customer does not have access to the applicable Customer Personal Data, PrimePay will (a) assist Customer by appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to a Data Subject Request under Applicable Data Protection Laws, and (b) PrimePay will, upon Customer's request and at Customer's expense, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent PrimePay is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws.

3.2 PrimePay Data Transfer Mechanism. For all transfers of EU Personal Data pursuant to the Agreement, the Parties hereby agree that the Data Privacy Framework shall constitute a valid transfer mechanism.

3.3 Prior Consultation. PrimePay agrees to provide reasonable assistance to Customer (at Customer's expense) where, in Customer's judgement, the type of Processing performed by PrimePay is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

3.4 Demonstrable Compliance. PrimePay agrees to keep records of its Processing of Customer Personal Data in compliance with Applicable Data Protection Laws and provide such records to Customer upon request.

4. INFORMATION SECURITY

PrimePay will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data, including those described in the Agreement and as required under Applicable Data Protection Laws.

5. ASSESSMENTS, AUDITS AND REMEDIATION

5.1 Assessments. Records to demonstrate compliance with this DPA and Applicable Data Protection Laws will be maintained by PrimePay and provided to Customer upon request. PrimePay will complete within two weeks any reasonable data protection questionnaire provided by Customer.

5.2 Audits. For the purpose of verifying PrimePay's compliance with Applicable Data Protection Laws and this DPA and upon reasonable notice of no less than thirty (30) days, PrimePay agrees to permit Customer, at Customer's cost and no more than once annually, to conduct audits through a PrimePay-approved third-party auditor. However, PrimePay agrees to allow audits to be conducted directly by Customer where, under Applicable Data Protection Laws, Customer is required to conduct audits directly. PrimePay agrees to cooperate in good faith with the audit and promptly (i) provide access to books, records (including, but not limited to, security scan records), systems, files, and other information necessary for the audit, and (ii) at Customer's request enable access to PrimePay's premises if absolutely necessary to properly conduct the audit or required under Applicable Data Protection Laws. Notwithstanding the

forgoing, Customer may not conduct any security scans or other intrusion testing on PrimePay's systems without the express prior written consent of PrimePay. Customer agrees to (x) schedule audits to minimize disruption to PrimePay's business, (y) require any third party it employs to sign a non-disclosure agreement, and (z) make the results of the audit available to PrimePay. Customer will only disclose the results of the audit to third parties to the extent such disclosure is (A) required to demonstrate Customer's own compliance, or (B) otherwise required under the Applicable Data Protection Laws.

5.3 Remediation. PrimePay agrees to promptly take action to correct any documented material security issue affecting Customer Personal Data identified by such audit and to inform Customer of such actions.

6. SECURE DISPOSAL

Customer Personal Data will be securely disposed (a) (i) during the term of the Agreement upon Customer's written request if such Customer Personal Data is no longer reasonably required to perform the Services, or (ii) at the termination of the provision of the Services in accordance with applicable law and/or PrimePay's Document Retention Policy, and (b) by deleting the Customer Personal Data or anonymizing such data. If instructed by Customer, a copy of such Customer Personal Data will be returned to Customer prior to disposal. PrimePay may retain Customer Personal Data to the extent that it is required to do so under Applicable Data Protection Laws.

7. CHANGES TO REQUIREMENTS

The Parties will work together in good faith to amend or supplement this DPA from time to time to reflect new requirements under Applicable Data Protection Laws.

8. SECURITY INCIDENT

8.1 Policy. PrimePay maintains reasonable Security Incident management policies and procedures and will, to the extent required under Applicable Data Protection Laws, notify Customer without undue delay after becoming aware of any Security Incident. PrimePay will make reasonable efforts to identify the cause of such Security Incident and take those steps as PrimePay deems necessary and reasonable in order to remediate the cause of such Security Incident to the extent the remediation is within PrimePay's reasonable control. The obligations in this Section shall not apply to Security Incidents that are caused by Customer or Customer's Users.

8.2 Reports. Upon request by Customer, PrimePay will enable Customer to review the results of and reports relating to the investigation and response to a Security Incident, which Customer will treat as Confidential Information of PrimePay.

9. TERMINATION OBLIGATIONS

Notwithstanding anything to the contrary in the Agreement or this DPA, Customer may terminate any Order Form, or any portion thereof, immediately upon written notice to PrimePay, and without judicial notice or resolution or prejudice to any other remedies, in the event a data protection or other regulatory authority or other tribunal or court in any country finds there has been a breach of Applicable Data Protection Laws by virtue of Customer's or PrimePay's Processing of Customer Personal Data in connection with the Agreement, and such breach has not been cured within thirty (30) days of PrimePay's receiving notice thereof.

10. LIMITATION OF LIABILITY

Without prejudice to any limitations afforded to data processors under any Applicable Data Privacy Laws, each party's liability arising out of or related to this DPA (whether in contract, tort or under any other theory of liability) is subject to the limitations of liability set forth in the Agreement; provided, in no event will such limitation apply to any Data Subject's rights under the DPF, SCCs or any Applicable Data Privacy Laws, as applicable.

11. CONTACT INFORMATION

PrimePay will designate a point of contact as its "**Privacy and Security Coordinator**". This Privacy and Security Coordinator will: (i) maintain responsibility for applying adequate protections to Customer Personal Data, including the development, implementation, and maintenance of its information security program, (ii) oversee application of PrimePay compliance with the requirements of this DPA, and (iii) serve as a point of contact for internal communications and communications with Customer pertaining to this DPA and compliance with or any breaches thereof.

In Witness Whereof, the Parties have caused this Data Processing Addendum to be executed as of the date executed by Customer.

[CUSTOMER NAME]	PRIMEPAY, LLC.
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____