DATA PROCESSING LAWS ADDENDUM

This Data Processing Laws Addendum ("Addendum") is attached to and made a part of the Agreement between FreedomPay ("FreedomPay", "Data Processor", "Service Provider" or "we") and Client, Reseller, or Customer ("Merchant", "Data Controller", "Business" or "you") ("Agreement"). The terms of the Addendum shall supersede the terms of the Agreement to the extent data protection obligations are covered.

Summary

This Data Processing Addendum (DPA) relates to the processing done by FreedomPay on behalf of Businesses/Data Controllers who engage in FreedomPay's Secure Switching Services. FreedomPay has taken all measures necessary to comply with existing Applicable Data Protection Laws, including but not limited to the **EU General Data Protection Regulation 2016/679 (GDPR), the UK retained version of the EU General Data Protection Regulation in The Data Protection Act of 2018 ("UK Act")**, and **TITLE 1.81.5. California Consumer Privacy Act of 2018 (CCPA)**. By executing the Agreement, Merchant engages FreedomPay to process certain data obtained by Merchant from consumers in the course of taking credit or debit card payment for selling goods or services to such consumers. This Addendum's purpose is to describe the roles, relationships and obligations of the parties involved under the Agreement with all Applicable Data Protection Laws in relation to FreedomPay's processing of data, and to ensure Data Processing is done in compliance of said Applicable Data Protection Laws. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Secure Switching Product Agreement or the meaning given to them in the Applicable Data Protection Law.

Definitions and Roles

Applicable Data Protection Laws

"Applicable Data Protection Laws" refers to any data protection, privacy legislation or industry requirements in the jurisdictions from which and to which the relevant Services are to be performed and as are amended from time to time, including but not limited to the **EU General Data Protection Regulation 2016/679 (GDPR), the UK retained version of the EU General Data Protection Regulation in The Data Protection Act of 2018** and **TITLE 1.81.5. California Consumer Privacy Act of 2018 (CCPA)**.

Personally Identifiable Information / Personal Data

"Personally Identifiable Information" or "Personal Data" may be used interchangeably and refers to any data provided to FreedomPay by, or at the direction of the Client as it relates to Consumers / Data Subjects in the course of the performance of the Secure Switching Product Agreement or other executed agreements. In general, Personally Identifiable Information or Personal Data means any information relating to an identified or identifiable natural person, or information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personally Identifiable Information or Personal Data retains the definitions given by way of any Applicable Data Protection Laws.

Examples of personal data that may be collected during the transaction process include, but are not limited to, name, credit card number, driver's license number, address, email address, telephone number, signature, consumer IP address, usernames, and banking information. Additional information may be collected and stored that when aggregated may constitute personally identifiable information as it could be reasonably linked, directly or indirectly with a particular consumer or household, including but not limited to, geographic data, purchasing indicators, business address, business telephone number, and web cookies.

Personally Identifiable Information is collected by FreedomPay, the Data Processor, on behalf of the FreedomPay Customer, the Data Controller, as part of the transaction process between the FreedomPay Customer and Consumer / Data Subject.

Data Subjects / Consumers

"Data Subjects" or "Consumers" may be used interchangeably and refers to identified or identifiable natural persons or households identified, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, 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.

As it relates to FreedomPay's services and solutions, the natural person making a payment to the Business using their credit or debit card to complete a transaction would be considered the Data Subject / Consumer.

Data Controller / Business

"Data Controller", "Business", and "Merchant" may be used interchangeably within the Agreement and are defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Merchants are classified as Data Controllers due to their role in accepting Personally Identifiable Information (PII) / Personal Data of their

consumers / data subjects, including full name and credit card Primary Account Number (PAN). Clients that do not fit the thresholds of a Business in California as defined under **Cal. Civ. Code Sec. 1798.140(c)(1)** will be considered Data Controllers for the purposes of this agreement as it relates to the responsibilities of determining the purpose and means of processing of personal data. Merchants should work with their internal compliance teams and/or 3rd party Data Protection Law and Regulation subject matter experts to ensure compliance with CCPA when processing payments within California, GDPR when processing data originating from the European Union, and the scope of all other Applicable Data Protection Laws. Merchants are also responsible for incoming requests from their qualifying Consumers / Data subjects, such as data disclosure and data deletion requests under CCPA if applicable, data erasure requests, data rectification, and data access under GDPR if applicable, and all further Consumer / Data Subject rights granted under Applicable Data Protection Laws.

Data Processor / Service Provider

"Data Processors" and "Service Provider" may be used interchangeably within the Agreement and are defined herein as a natural or legal person, public authority, agency, company or other body which processes personal data on behalf of the controller.

FreedomPay acts as a Data Processor / Service Provider on behalf of its Merchants due to FreedomPay's processing activities, specifically, transaction routing and tokenization. The Secure Switching Product Agreement outlines the permitted purposes of the personal information collected and the services that the Merchant has contracted the FreedomPay to perform, in conjunction with any other Agreement or Addendum on file between the Merchant and FreedomPay. The Data Controller and Data Processor relationship is undertaken pursuant to the written Agreement, where the Agreement prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by Applicable Data Protection Laws, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business. FreedomPay's obligations as a Data Processor / Service Provider are defined within section "FreedomPay's Obligations as a Data Processor / Service Provider."

Subprocessors

"Subprocessors" are any third-party data processors used by FreedomPay to fulfill data processing obligations set under the Agreement.

Merchants Must Comply with Applicable Data Protection Laws and Regulations

Merchants are required to comply with Applicable Data Protection Laws. Merchants should seek independent guidance on becoming compliant with Applicable Data Protection Laws and determining what data protection laws are applicable to the Merchant. Although FreedomPay complies with Applicable Data Protection Laws through its processing activities, Merchants must also comply with Applicable Data Protection Laws independently.

Data Requests from Data Subjects / Consumers

As a Data Controller, Merchants may receive requests from their customers regarding the management of their data, required under Applicable Data Protection Laws such as GDPR, UK Act and CCPA . Data Requests include data disclosure and data deletion requests under CCPA, data erasure requests, data rectification, and data access under GDPR and/or the UK Act, and all further Consumer / Data Subject rights for data management and notification granted under Applicable Data Protection Laws. FreedomPay can support Data Requests from its Merchants, but it is required that the identity of the customer has been validated by the Merchant (Controller) prior to issuing the request. Merchants must interact directly with the Data Subject, and then initiate any requests to FreedomPay on behalf of the Data Subject based on FreedomPay's classification as a Data Processor. To initiate requests for the management of consumer data, Merchants must complete the form attached to this amendment and submit to techsupport@freedompay.com. FreedomPay will acknowledge the request, and provide you updates on the status of the request, including the final resolution or decision on the request. As the Data Controller, you must communicate with the Data Subject / Consumer accordingly.

FreedomPay's Obligations as a Data Processor / Service Provider

This section constitutes written instruction from the Data Controller/Merchant for FreedomPay to process customer information for the purposes of transaction routing and tokenization. FreedomPay agrees to inform Merchant if it cannot comply with processing instruction either operationally or legally. FreedomPay will not process the Merchant's customer data for any purpose other than for the specific purpose specified in the Agreement or Addendum without first amending the Agreement and this Addendum. FreedomPay agrees that all Merchant's customer data is the property of Merchant.

1. The collection and processing of customer information and access of Merchant's systems is limited to what is necessary to perform the documented "business purpose" for which FreedomPay was retained as specified in the Agreement or Addendum, where the use is (i) "reasonably necessary and proportionate" to achieve the operational purpose for which it was collected or processed, or (ii) for another operational purpose that is compatible with the context in which it was collected. This may include detecting security

incidents, debugging errors that impair functionality, undertaking activities to verify or maintain the quality or safety of, or to upgrade or enhance, a Business' service, undertaking internal research for technological development and demonstration, performing services such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the Merchant as specified in the Agreement or Addendum and in accordance with Applicable Data Protection Laws. FreedomPay agrees not to retain, use or disclose the Merchant's customer data or Personal Data for any purpose other than for the purpose outlined above, including retaining, using, or disclosing the Merchant's customer data for a commercial purpose other than performing the services specified in this Addendum or the Agreement. Any such data that is de-identified and aggregated with other data such that the consumer and the Merchant cannot be identified shall not be subject to the previous sentence.

2. FreedomPay will immediately inform the Merchant if, in FreedomPay's opinion, an instruction given to FreedomPay infringes upon Applicable Data Protection Laws.
3. Merchant agrees that FreedomPay may engage Subprocessors as required to accomplish the processing activities. FreedomPay will only engage Subprocessors with the same or greater contractual obligations as exist between the Merchant and FreedomPay. FreedomPay agrees to keep a list of subprocessor agreements which shall be updated regularly and made available to Merchant upon reasonable request. FreedomPay shall give Merchant prior written notice of the appointment of any subprocessor including full details of the processing by the subprocessor. FreedomPay agrees that it shall be liable for the failure of the sub processor to fulfill its obligations, to the extent that FreedomPay would be liable under the Agreement if FreedomPay performed the processing. For all transaction routing/processing services, FreedomPay is required to pass transactional data to the Merchant's processor/acquiring bank to provide its services.
    a. In addition to Merchant's processor/acquiring bank, FreedomPay will provide Merchant's data to additional Subprocessors as requested by the Merchant, or as necessary to accomplish the processing, as described below. FreedomPay will accept these requests through its standard Boarding processes and procedures and will consider the submission of the appropriate Boarding forms as consent to send data to Merchant's specific Subprocessors. This may include gift card providers, fraud management, chargeback management or other payment solution providers. Merchant agrees that submission of the appropriate intake forms (e.g., Boarding forms) to provide data to Merchant's Subprocessor serves as Merchant's consent to provide data to said Subprocessors as it relates to FreedomPay Data Processing Activities of transaction processing and tokenization.
4. All FreedomPay personnel with responsibilities affecting processing of personal data have received training specific to their obligations pertaining to those processing activities and the requirements of Applicable Data Protection Laws and Regulations and have formally acknowledged their responsibilities. All persons authorized to process the personal data are under an appropriate obligation of confidentiality.
5. FreedomPay has implemented appropriate physical, technical and organizational security measures to protect data provided to FreedomPay as a Data Processor against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access, including encryption, ongoing audits and security reviews, redundancy and back-up facilities, and regular security testing. To the extent that PCI is applicable to FreedomPay, it agrees to fully comply with PCI standards and provide, upon request, an attestation of compliance completed by a qualified assessor annually.
6. FreedomPay will assist the Data Controller/Merchant with its compliance obligations regarding the rights of Data Subjects related to FreedomPay's processing activities, as per the Data Subject Request Form. FreedomPay agrees to notify Merchant promptly about any requests, inquiries or complaints received about the processing of Merchant's customer data or Personal Data from third parties such as law enforcement, legal authorities and Data Subjects. FreedomPay agrees to assist with responding to Data Subject requests within a timeline that allows Merchant to meet its legal obligations. FreedomPay shall not respond to any such requests without first consulting with Merchant.
7. FreedomPay will assist the Data Controller/Merchant in complying with obligations regarding security and prior consultation with data protection authorities before undertaking high risk processing as it pertains to the data processing operations FreedomPay conducts on the controller/Merchant's behalf. This entails maintaining security controls over the in-scope environment (i.e. PCI/P2PE certification, etc.). FreedomPay isn't involved in "high risk" processing.
8. Subject to Applicable Data Protection Laws and Regulations, FreedomPay will notify the Data Controller/Merchant of a data breach promptly without undue delay.
9. FreedomPay agrees to delete or return the Data Controller/Merchant's data, but not any cardholder or cardholder related data, on termination of the agreement. If FreedomPay cannot feasibly return or destroy any Merchants customer data or Personal Data it shall hold such data according to the terms of this Addendum and not use it for any purpose and return or destroy in accordance with FreedomPay's normal policies.
10. FreedomPay agrees to provide the Data Controller/Merchant with information necessary to prove compliance with all regulations and to cooperate with supervisory authorities as required, to the extent involving FreedomPay's processing activities, and will allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller to demonstrate compliance with and where required by Applicable Data Protection Laws.

11. FreedomPay agrees to notify Merchant within 72 hours upon learning with reasonable certainty of a security breach. FreedomPay agrees to cooperate fully in investigating, remediating any harms, implementing corrective actions. FreedomPay agrees to take full responsibility and subject to the limitations in the Agreement, bear all costs associated with a security breach as a result of their negligence or breach of requirements under this Addendum.

12. FreedomPay agrees not to process Merchant's customer data or Personal Data in a jurisdiction outside of the jurisdiction in which it was collected without the written consent of Merchant.

13. FreedomPay agrees to maintain a record of processing activities pertaining to Merchant's customer data or Personal Data including relevant details such as categories of processing, cross-border transfers carried out on behalf of Merchant. FreedomPay agrees to make records of processing available to Merchant and any relevant government authority upon reasonable request.

Indemnification by Merchant. Merchant shall indemnify, defend and hold harmless FreedomPay and its affiliates, officers, directors and employees (as applicable, "**Indemnitees**") from any and all losses, damages, costs and expenses (including reasonable attorneys' fees and costs) (together, "**Losses**") arising from or in connection to any claim, action, proceeding (together, "**Claims**") asserted against such Indemnitee(s) by a third party asserting any violation of Applicable Data Protection Laws to the extent caused by the actions of Merchants or any Subprocessors to whom FreedomPay sends data either at the Merchant's request or requirement, or because it was necessary to complete the processing. The limitations of liability set forth in the Agreement shall not apply to any such Losses.

APPENDIX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR (or as applicable, equivalent provisions of any other Data Protection Law).

Subject matter and duration of the Processing of Customer Personal Data

The subject matter of the Processing of the Customer Personal Data is set out in the Secure Switching Product Agreement and this Addendum.

The duration of processing of customer data is 10 years to comply with the longest statute of limitations for financial data within the EU.

The nature and purpose of the Processing of Customer Personal Data

Nature:

- Collection
- Deletion
- Disclosure
- Use

Purpose:

Customer Personal Data is used to complete secure switching transactions as set out in the Secure Switching Product Agreement.

The types of Customer Personal Data to be Processed

- Customer Data of natural persons

The categories of Data Subject to whom the Customer Personal Data relates

Special Categories of Personal Data (Art. 9 GDPR)

- None

The obligations and rights of Controller and Controller Affiliates

The obligations and rights of Controllers and Controller Affiliates are set out in the Secure Switching Product Agreement and this Addendum.

APPENDIX 2: DATA SUBJECT REQUEST FORM

Summary

Depending on Applicable Data Protection Laws, the Data Subject / Consumer may have the right to exercise certain rights concerning their personal data. Merchants, acting as the Data Controller or Business, should determine what requests are valid under Applicable Data Protection Laws such as GDPR, UK Act and CCPA, and should handle requests independently of

FreedomPay based on their obligations to the consumer as a Data Controller processing personal data. As a Data Processor, FreedomPay can provide additional information as it relates to the data that FreedomPay is processing on behalf of the data subject. Merchants may submit a request to FreedomPay on behalf of the data subject for information on the data that FreedomPay is processing.

Requests for data will be handled through FreedomPay's support team. Requests can be made via email or phone by contacting techsupport@freedompay.com or 888.495.2446. Please be prepared to provide the following information to FreedomPay Support to initiate this request.

i. Merchant Name: _____

ii. Consumer Name: _____

iii. Client ID _____

iv. Store ID: _____

v. Request ID: _____

vi. Last four digits of card number: _____