AUTHORIZE.NET DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is an agreement between you and the entity you represent ("Customer" or "you"), on the one hand, and Authorize.Net LLC ("Authorize.Net"), on the other hand. It forms part of any written or electronic agreement between you and Authorize.Net under which Authorize.Net Processes Personal Information on your behalf (each, an "Agreement"), except with respect to any Agreement under which you and Authorize.Net have entered data processing terms that address the subject matter hereof. This DPA forms a part of the Services Documentation, defined in the Agreement.

1 Processing of Customer Personal Information

1.1 **Processor designation**. The parties acknowledge and agree that with respect to the Customer Personal Information that Authorize.Net Processes to provide the Transaction Services, which Processing may include, by way of example and for illustrative purposes the Processing detailed on Details of Processing Customer Personal Information (Exhibit 2), that Authorize.Net is a "processor" or "service provider" under Applicable Data Protection Laws acting on Customer's instructions (referred to as "Processor" for purposes of this DPA).

1.2 **Authorization to Process**. Processor will Process Customer Personal Information to provide such Transaction Services, and Processor is authorized to Process Customer Personal Information solely in connection with the following activities:

1.2.1 In accordance with the applicable Agreement(s), including, without limitation, any exhibits, schedules, and applicable price schedule(s), to provide the Transaction Services, and any Processing required under applicable law or regulations;

1.2.2 Based on the instructions of Customer and in its use of the Transactions Services, Authorize.Net will transfer Customer Personal Information to acquiring banks, issuing banks, payment processors providing services on behalf of acquiring banks, credit/debit card companies, or service providers performing payer authentication services used by Customer, such as Verified by Visa and Mastercard Identity Check (ID Check);

1.2.3 As reasonably necessary to enable Authorize.Net to comply with any other directions or instructions provided by Customer; and

1.2.4 To support the creation of models for Authorize.Net's security and fraud prevention tools for use by the Customer and/or any other customer of Authorize.Net. These models ensure Customer is provided with the most up to date scoring as part of the Transaction Services.

2 **Compliance with Law**. Each of Authorize.Net, in its provision of services to Customer, and Customer, in its use of the services, shall Process Customer Personal Information in accordance with Applicable Data Protection Law.

3 Customer obligations

3.1 Customer shall provide its End-User(s) with all privacy notices, information and any necessary choices and shall obtain any necessary consents to enable the parties to comply with Applicable Data Protection Law;

3.2 Where required by Applicable Data Protection Law, Customer shall promptly inform Processor when Customer Personal Information must be corrected, updated, and/or deleted;

3.3 Customer shall ensure that at the point of transferring Customer Personal Information to Processor, the Customer Personal Information is adequate, relevant and limited to what is necessary in relation to the Processing envisaged under the Agreement and this DPA; and

3.4 Customer shall comply (and ensure that its third party auditor's comply) with Processor's relevant security policies and appropriate confidentiality obligations as set out in the Agreement.

4 Authorize.Net obligations

4.1 **Applicable Data Protection Law**. To the extent necessary to enable Customer to comply with its obligations under Applicable Data Protection Law, Authorize.Net further agrees to comply with any required provisions of the GDPR Schedule (other than when acting in accordance with Section 1.2 (Authorization to Process) of this DPA) and/or CCPA Schedule, each, to the extent applicable.

4.2 **Data Subject Rights**. Processor will, to the extent legally permitted, provide reasonable assistance to Customer to respond to requests from End-Users to exercise their rights under Applicable Data Protection Law (e.g., rights to access or delete Personal Information) in a manner that is consistent with the nature and functionality of the Transaction Services. Where Authorize.Net receives any such request, it shall notify Customer and the Customer is responsible for handling such requests by an End User in accordance with Applicable Data Protection Law.

4.3 **Engaging with Sub-Processors**. Processor shall ensure that when engaging with another data processor including any Affiliates (a "Sub-Processor") for the purposes of carrying out specific Processing activities on behalf of Customer, there is a written contract in place between Processor and the relevant Sub-Processor. Such written contracts, to the extent applicable to the nature of the Transaction Services provided by the relevant Sub-Processor, will provide at least the same level of protection for Customer Personal Information as set out in this DPA.

4.4 **Staff**. Processor shall ensure that persons authorized to Process Customer Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.5 **Security of Processing**. 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, Processor shall implement technical and organizational measures to ensure a level of security appropriate to that risk. In assessing the appropriate level of security, Processor shall, in particular, take into account the risks that are presented by the Processing, in particular from unauthorized or unlawful Processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Information transmitted, stored or otherwise Processed. Processor shall provide reasonable assistance to Customer in ensuring Customer meets its own compliance obligations with respect to these same security measures.

4.6 Security Breach

4.6.1 In the event of an actual Security Breach (defined below) affecting Customer Personal Information contained in Processor's systems, Processor shall (i) investigate the circumstances, extent and causes of the Security Breach and report the results to Customer and continue to keep Customer informed on a regular basis of the progress of Processor's investigation until the issue has been effectively resolved; and (ii) cooperate with Customer in any legally required notification by Customer of affected End-Users. The obligations herein shall not apply to Security Breaches caused by Customer or Customer's End-Users.

4.6.2 Processor shall notify Customer without undue delay upon Processor or any Sub-Processor becoming aware of an actual Security Breach affecting Customer Personal Information, providing the Customer with sufficient information and reasonable assistance to allow Customer to meet its obligations under Applicable Data Protection Law to (i) notify a Supervisory Authority (as defined under Applicable Data Protection Law) of the Security Breach; and (ii) communicate the Security Breach to the relevant Data Subjects.

4.6.3 Notice to Customer in accordance with Section 4.6.2 of this Agreement shall be made by sending an email and/or text message to the email address and/or mobile phone number registered by Customer in the Authorize.Net Merchant Interface

4.6.4 Except as required by applicable law or regulation, the notifying party will not make (or permit any third party to make) any statement concerning the Security Breach that directly or indirectly references the other party, unless the other party provides its explicit written authorization.

4.7 Deletion and Retention. Processor shall, at the choice of Customer, delete or return all Customer Personal Information upon termination of the Agreement and delete existing copies unless storage is required by applicable law.

5 Miscellaneous. The terms of this DPA shall apply only to the extent required by Applicable Data Protection Law. To the extent not inconsistent herewith, the applicable provisions of the Agreement(s) (including without limitation, indemnifications, limitations of liability, enforcement, and interpretation) shall apply to this DPA. In the event of any conflict between this DPA and the terms of an applicable Agreement, the terms of this DPA shall control solely with respect to data processing terms where required by Applicable Data Protection Law, and, in all other respects, the terms of the applicable Agreement shall control. Notwithstanding any term or condition of the DPA, the DPA does not apply to any data or information that does not relate to one or more identifiable individuals, that has been aggregated or de-identified in accordance with Applicable Data Protection Law, or to the extent that Authorize.Net and you have entered separate data processing terms that address the subject matter hereof.

6 Definitions. Unless otherwise defined in the Agreement (including this DPA), all terms in this DPA shall have the definitions given to them in Applicable Data Protection Law.

6.1 "Applicable Data Protection Law" means any law or regulation pertaining to data protection, privacy, and/or the Processing of Personal Information, to the extent applicable in respect of a party's obligations under the Agreement and this DPA. For illustrative purposes only, Applicable Data Protection Laws include, without limitation, and to the extent applicable, the General Data Protection Regulation (Regulation (EU) 2016/679 (the "GDPR"), the UK Data Protection Act 2018, the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. ("CCPA"), and any associated regulations or any other legislation or regulations that transpose or supersede the above;

6.2 "Customer Personal Information" means Personal Information originating from the Customer or its End-Users and provided to or accessed by Authorize.Net pursuant to the Agreement;

6.3 "End-User(s)" means any person that purchases goods or services of Customer, whose information is submitted by Customer to Authorize.Net during the course of Customer using the Transaction Services hereunder;

6.4 "Personal Information" means all data or information, in any form or format, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer ("Data Subject") or household or that is regulated as "personal data,"

"personal information," or otherwise under Applicable Data Protection Law. For the avoidance of doubt, this includes any information relating to an End-User as defined in the Agreement;

6.5 "Process" or "Processed" or "Processing" means any operation or set of operations which is performed upon Personal Information , whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, disclosure or otherwise making available, duplication, transmission, combination, blocking, redaction, erasure or destruction; and

6.6 "Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information. A Security Breach includes a "personal data breach" (as defined in the GDPR), a "breach of security of a system" or similar term (as defined in any other applicable privacy laws) as well as any other event that compromises the security, confidentiality or integrity of Personal Information.

SCHEDULE A
CALIFORNIA CONSUMER PRIVACY ACT

This CCPA Schedule applies in addition to any terms set forth in the body of the DPA (and is incorporated therein) when the CCPA applies to your use of Transaction Services. Capitalized terms not defined herein have the meaning assigned to them under the DPA. To the extent there are any conflicts between this CCPA Schedule and the DPA, this CCPA Schedule shall prevail.

1 Authorize.Net shall not:

1.1 sell Customer Personal Information; or

1.2 retain, use or disclose Customer Personal Information other than as set forth in the body of the DPA, except as required or permitted by Applicable Data Protection Law.

2 When providing or making available Personal Information to Authorize.Net, Customer shall only disclose or transmit that Personal Information which is necessary for Authorize.Net to perform its obligations under the applicable Agreement(s).

3 To the extent required by Applicable Data Protection Law, this CCPA Schedule constitutes its certification to the Processing restrictions herein.

SCHEDULE B
GENERAL DATA PROTECTION REGULATION

This GDPR Schedule applies in addition to any terms set forth in the body of the DPA (and is incorporated therein) when the GDPR applies to your use of Transaction Services. Capitalized terms not defined herein have the meaning assigned to them under the DPA. To the extent there are any conflicts between this GDPR Schedule and the DPA, this GDPR Schedule shall prevail.

1 Processor Obligations

1.1 Processing of Customer Personal Information. Processor shall Process Customer Personal Information only on documented reasonable instructions from Customer (including instructions with respect to transfers of Customer Personal Information to a third country, if applicable) unless required to do so by Applicable Data Protection Law. In such circumstances, Processor shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

1.2 Use of Sub-Processor

1.2.1 Processor shall not engage any Sub-Processor without the specific or general written authorization from Customer.

1.2.2 In the case of a general authorization, Processor shall inform Customer of any intended changes concerning the addition or replacement of other Sub-Processors to give Customer the reasonable opportunity to object to such changes. In the event Customer objects to Processor's change or addition of Sub-Processor, Customer shall promptly notify Processor of its objections in writing within 10 business days after receipt of Processor's notice of such change or addition.

1.2.3 Processor may, at its option, undertake reasonable efforts to make available to Customer a change in the Transaction Services or recommend a commercially reasonable change to Customer's configuration or use of the Transaction Services to avoid Processing of Customer Personal Information by the objected-to new Sub-processor. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the Agreement with respect to only those aspects of the Transaction Services, which cannot be provided by Processor without the use of the objected-to new Sub-processor by providing written notice to Processor. If the Transaction Services as a whole cannot be performed without the objected-to new Sub-Processor, Customer may terminate the entire Agreement.

1.2.4 Processor agrees not to impose a penalty for any termination under Section 1.2.3 of this GDPR Schedule on Customer. Processor reserves the right to maintain its Sub-Processor list through means such as publication of its Sub-Processor list online. In accordance with Section 1.2.1 of this GDPR Schedule, Customer provides authorization for Processor to engage with the Sub-Processors listed in the Authorize.Net Merchant Interface.

2 Data Protection Impact Assessments and Prior Consultation with Regulator

2.1 Processor shall immediately inform Customer if, in Processor's opinion, Customer's instructions would be in breach of Applicable Data Protection Law. Customer agrees that Processor shall be under no obligation to take actions designed to form any such opinion.

2.2 Processor shall provide reasonable assistance to Customer with any legally required (a) data protection impact assessments; and (b) prior consultations initiated by the Customer with its regulator in connection with such data protection impact assessments. Such assistance shall be strictly limited to the Processing of Customer Personal Information by Processor on behalf of Customer under the

Agreement taking into account the nature of the Processing and information available to the Processor.

3 Demonstrating Compliance with this DPA

3.1 Processor shall make available to Customer all information necessary to demonstrate compliance with its obligations under this DPA and allow for (and contribute to) audits, including inspections conducted by Customer or another auditor under the instruction of the Customer for the same purposes of demonstrating compliance with obligations set out in this DPA.

3.2 Customer's right under Section 3.1 of this GDPR Schedule is subject to the following:

3.2.1 if Processor can demonstrate compliance with its obligations set out in this DPA by adhering to an approved code of conduct, by obtaining an approved certification or by providing Customer with an audit report issued by an independent third party auditor (provided that Customer will comply with appropriate confidentiality obligations as set out in the Agreement and shall not use such audit report for any other purpose), Customer agrees that it will not conduct an audit or inspection under Section 3.1 above;

3.2.2 in acknowledgement of the time, expense and disruption to business associated with performing audits and inspections involving interviews and onsite visits, Customer agrees to only conduct such audits and inspections on condition that Customer can demonstrate such audit or inspection is necessary beyond the information made available by Processor under Section 3.1 above. Such audits and inspections, shall be at reasonable intervals (but not more than once per year) upon not less than 60 days' notice and at a date mutually agreed by the Parties, provided that the audit will (i) not disrupt Processor's business; (ii) be conducted during business hours and at the Customer's expense; (iii) not interfere with the interests of Processor's other customers; and (iv) not exceed a period of two successive business days.

4 Cross-Border Transfers

4.1 Processor shall comply with Customer's documented instructions concerning the transfer of Customer Personal Information to a third country.

4.2 The Processor shall only Process or otherwise transfer any Customer Personal Information outside the European Economic Area ("EEA"), the UK or Switzerland in compliance with the Applicable Data Protection Law unless otherwise required by applicable law to which the Processor is subject; in such case, the Processor shall inform Customer of that legal requirement before undertaking such processing of Customer Personal Information unless such applicable law prohibits such information on important grounds of public interest.

4.3 Customer agrees and acknowledges that Processor transfers and stores certain Customer Personal Information (relating to individuals located in the EEA) in the United States.

4.4 The controller to processor standard contractual clauses (as set out in Commission Decision C(2010)593 dated 5 February 2010 made under Directive 95/46/EC of the European Parliament and of the Council as amended or superseded from time to time) (the "C2P Standard Contractual Clauses") apply with respect to any transfer of Customer Personal Information to Authorize.Net and any of its affiliated entities in the United States or other third countries ("Authorize.Net Entities"). The parties acknowledge and agree that:

4.4.1 the C2P Standard Contractual Clauses are hereby incorporated by reference;

4.4.2 Customer and any of its commonly owned or controlled affiliates that have signed an Agreement for Transaction Services ("Customer Entities") shall be deemed to be "data exporters" for purposes of the C2P Standard Contractual Clauses;

4.4.3 the Authorize.Net Entities shall be the "data importer" for the purposes of the C2P Standard Contractual Clauses;

4.4.4 the Customer Entities and the Authorize.Net Entities shall each comply with their respective obligations in the C2P Standard Contractual Clauses;

4.4.5 if there is any conflict or inconsistency between a term in the body of this DPA, an Agreement and a term in the C2P Standard Contractual Clauses incorporated into this DPA, the term in the C2P Standard Contractual Clauses shall take precedence; and

4.4.6 the parties agree that the information Annex 1 of this GDPR Addendum is incorporated into Appendices 1 and 2 of the C2P Standard Contractual Clauses.

EXHIBIT 1
INFORMATION REQUIRED FOR THE C2P STANDARD CONTRACTUAL CLAUSES

Information to be incorporated into Appendix 1 of the C2P Standard Contractual Clauses	
Category of Information Required by Appendix 1 of the C2P Standard Contractual Clauses	Information Agreed by the Parties
Data Exporter	Customer Entities
Data Importer	Authorize.Net Entities
Data Subjects	As set out in the table in Exhibit 2 under "Categories of Data Subjects".
Categories of Data	As set out in the table in Exhibit 2 under "Types of Personal Information".
Special Categories of Data	Not Applicable
Processing Operations	As set out in the table in Exhibit 2 under "Nature and Purpose of the Processing".
Information to be incorporated into Appendix 2 of the C2P Standard Contractual Clauses	
Category of Information Required by Appendix 2 of the C2P Standard Contractual Clauses	Information Agreed by the Parties
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached)	Authorize.Net is certified as compliant with all standards established by the Payment Card Industry Data Security Standards (together with any successor organization thereto, "PCI DSS") that are applicable to Authorize.Net and its affiliates (such standards, the "PCI Standards"). As evidence of compliance, Customer may access Authorize.Net's current Attestation of Compliance signed by a Payment Card Industry Qualified Security Assessor through Visa Online. Authorize.Net maintains and enforces commercially reasonable information security and physical security policies, procedures and standards, that are designed (i) to insure the security and confidentiality of Customer's records and information, (ii) to protect against any anticipated threats or hazards to the security or integrity of such records, and (iii) to protect against unauthorized access to or use of such records or information which could result in substantial harm (the "Visa Information Security Program"). At a minimum, the Visa Information Security Program is designed to meet the standards set forth in ISO 27002 published by the International Organization for Standardization,

	as well as any revisions, versions or other standards or objectives that supersede or replace the foregoing. Authorize.Net engages its independent certified public accountants to conduct a review of Authorize.Net's operations and procedures at Authorize.Net's cost. The accountants conduct the review in accordance with the American Institute of Certified Public Accounts Statement on Standards for Attestation Engagements No. 18 SOC I Type II ("SSAE 18") and record their findings and recommendations in a report to Authorize.Net. Upon request, and subject to standard confidentiality obligations, Authorize.Net will provide its most recent SSAE 18 and, in Authorize.Net's reasonable discretion, additional information reasonably requested to address questions or concerns regarding the SSAE 18's findings.

EXHIBIT 2
DETAILS OF PROCESSING CUSTOMER PERSONAL INFORMATION

Service	Nature and purpose of the processing	Types of personal information	Categories of data subjects to whom the personal information relates to
Advanced Fraud Detection Suite (AFDS) and Fraud Detection Suite (FDS)	AFDS & FDS provide the Customer with risk management and fraud screening services. Personal Information is used to mitigate fraud on the Customer and Consumers behalf based on the instructions of the Customer or Authorize.net.	Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address, and IP address may be used. Further detail is included in the applicable Services Documentation.	End-Users as defined under the Agreement (including credit card holders, bank transfer users, direct debit users, all end users whose cardholder or bank account data is submitted to Processor for processing).
Recurring Billing	Recurring Billing provides a service that captures recurring payments with cards on file.	If the Customer opts to use Recurring Billing, we may use Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address. Further detail is included in the applicable Services Documentation,	
Account Updater	Account Updater is a service that automatically updates account numbers and expiration dates for cards on file in Recurring Billing subscriptions & Customer Information Manager (CIM) profiles.	If the Customer opts to Account Updater, we may use Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address.	

		Further detail is included in the applicable Services Documentation.	
Invoicing	Invoicing is a service that emails a digital invoice to a customer and can accept digital payments for goods and services.	If the Customer opts to use Invoicing, we may use Cardholder and banking information, including, without limitation, card numbers, email, name, address. Further detail is included in the applicable Services Documentation.	
Payment Gateway	Gateway services for bank transfers, direct debits, credit/debit card authorisation, settlement, authentication and credit, including processing, provision of customer support.	Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address. Further detail is included in the applicable Services Documentation.	