Data Processing Addendum
Effective Date: November 20, 2024

Drive Commerce, LLC, a Delaware limited liability company with offices at 500 Westover Dr #31793, Sanford, NC 27330, and the customer ("Customer") agreeing to these terms have entered into a Master Services Agreement, Services Agreement, or other written or electronic agreement for Drive Commerce's provision of Services to Customer (the "Agreement").

This Data Processing Addendum (the "Addendum") forms part of the Agreement, where in connection of the provision of Services to Customer, Drive Commerce Processes Personal Data on behalf of Customer.

For purposes of this Addendum, the parties agree that Drive Commerce ("Data Processor") is a Data Processor and Customer ("Data Controller") is the Data Controller under Applicable Privacy Laws for the purposes of processing Personal Data pursuant to the Agreement. Terms not otherwise defined in this Addendum shall have the meaning set forth in the Agreement, and capitalized terms that are undefined shall have the meanings ascribed to them under Applicable Privacy Laws.

This Addendum will be effective from the date on which the parties agreed to this Addendum, will remain in force and effect until the Agreement has been terminated or expires, and will replace and supersede any previously applicable terms relating to their subject matter. In the event of any conflict of inconsistency with the terms of the Agreement, this Addendum will take precedence over the terms of the Agreement; provided, however, that where a separate data protection clause forms part of the Agreement, the most stringent applicable data protection term shall apply.

1. DEFINITIONS

1.1. "**Affiliate(s)**" means an entity directly or indirectly controlling, controlled by or under common control with such party. "Control" shall mean, with respect to any entity, the right to exercise or cause the exercise of at least fifty percent (50%) of the voting rights in such entity.

1.2. **"Applicable Privacy Laws"** means all international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security of Personal Data relating to the Data Subjects Processed by Data Processor pursuant to the Agreement, including without limitation and applicable United States Data Protection Laws and European Data Protection Laws.

1.3. "**Artificial Intelligence**" means any computer software, system, or model developed through machine, deep learning, neural networks, natural language processing, robotics, or related techniques, which can perform tasks that simulate human intelligence such as learning, reasoning, problem-solving, perception, prediction, interaction, and autonomy.

1.4. “**Data Subject**” means any individual to whom Personal Data relates.

1.5. **“Europe"** means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

1.6. **“European Data”** means Personal Data that is subject to the protection of European Data Protection Laws.

1.7. **"European Data Protection Laws"** means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

1.8. **“Personal Data**” means any personal information, as defined by Applicable Privacy Laws, relating to an identified or identifiable individual, that is:

1.8.1. disclosed at any time to Data Processor or its Personnel by Data Controller or its Personnel in anticipation of, in connection with or incidental to the performance of services for or on behalf of Data Controller;

1.8.2. Processed (as defined below) at any time by Data Processor or its Personnel in connection with or incidental to the performance of services for or on behalf of Data Controller; or

1.8.3. derived by Data Processor or its Personnel from the information described in (i) and (ii) above.

1.9. “**Personnel**” means any employees, agents, consultants, contractors, Sub-Processors, or service providers of Data Processor or Data Controller, as appropriate.

1.10. “**Process**” or “**Processing**” means any operation or set of operations performed upon Personal Data, whether or not by automatic means, including, without limitation, creating, collecting, aggregating, procuring, obtaining, accessing, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, aligning, combining, restricting, erasing and/or destroying the information.

1.11. **“Regulated United States Data”** shall mean Personal Data Processed pursuant to the Agreement and this Addendum that is regulated by United States Data Protection Laws

1.12. **“Regulator”** means any entity which has jurisdiction to enforce Data Controller and Data Processor’s compliance with the Applicable Privacy Laws.

1.13. A **“Security Incident”** has occurred when Data Processor has knowledge of or reasonably believes there has been unauthorized access and exfiltration, theft, or disclosure, or any other compromise of Personal Data within the possession or control (e.g., physical or IT environment) of Data Processor or any Personnel.

1.14. “**Services”** shall refer to all services and solutions provided to Data Controller pursuant to the Agreement.

1.15. “**Standard Contractual Clauses**” means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021 currently found at https://eur-lex.europa.eu/eli/dec_impl/2021/914, as may be amended, superseded or replaced.

1.16. “**Sub-Processor”** means an entity engaged or appointed by Data Processor (or any other Sub-Processor) to Process Personal Data on behalf of Customer in connection with the Agreement.

1.17. “**United States Data Protection Laws**” means all United States federal and state laws and regulations applicable to the processing of Personal Data under the Agreement, including (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 and its implementing regulations (collectively, the “CCPA”), (b) the Virginia Consumer Data Protection Act (c) the Colorado Privacy Act and its implementing regulations, (d) the Utah Consumer Privacy Act; (e) the Connecticut Data Privacy Act; (d) the Oregon Consumer Privacy Act; (e) the Texas Data Privacy and Security Act; (f) the Utah Consumer Privacy Act; (g) the Virginia Data Protection Act; and (h) when effective, the Delaware Personal Data Privacy Act, the Indiana Consumer Data Protection Act, the Iowa Consumer Data Protection Act, the Kentucky Consumer Data Protection Act, the Maryland Online Data Privacy Act, the Minnesota Consumer Data Privacy Act, the Montana Consumer Data Privacy Act, the Nebraska Data Privacy Act, New Hampshire SB 255, New Jersey SB 332, the Rhode Island Data Transparency and Privacy Protection Act, and the Tennessee Information Protection Act.

2. PRIVACY, CONFIDENTIALITY AND PERSONAL DATA SECURITY

2.1. Data Controller's Covenants and Obligations

2.1.1. Data Controller warrants that it has all necessary rights to provide the Personal Data to the Data Processor for the Processing to be performed pursuant to the Agreement, and that no applicable law, or legal requirement, or privacy or information security enforcement action, investigation, litigation or claim, or any other circumstance, prohibits Data Controller from (i) fulfilling its obligations under this Addendum, or (ii) providing instructions to Data Processor concerning Personal Data (the "Instructions").

2.1.2. Data Controller has the exclusive authority to determine the purposes and means of Processing of all Personal Data subject to this Addendum, the Agreement and any related agreements.

2.1.3. Within the scope of the Agreement and in its use of the services, Data Controller will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to Data Processor. In particular but without prejudice to the generality of the foregoing, Data Controller acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which Data Controller acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including the provision of necessary privacy notices, and obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes); (iii) ensuring Data Controller has the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); and (iv) ensuring that Data Controller's Instructions to Data Processor regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws. Data Controller will inform Data Processor without undue delay if Data Controller is not able to comply with its responsibilities under applicable Data Protection Laws. Without limiting the foregoing, Data Controller specifically acknowledges that its use of the Services will not violate the rights of any Data Subject in regards to the use of Artificial Intelligence as included in the Instructions as part of the requested Services, and that Data Controller has obtained all proper permission for use of a Data Subject's name, image, and/or likeness pursuant to the Instructions as part of the requested Services.

2.1.4. The parties agree that the Agreement (including this DPA) constitutes Data Controller's complete Instructions to Data Processor in relation to the Processing of Personal Data, provided that Data Controller may provide additional instructions that are consistent with the Agreement. Data Controller shall disclose Personal Information to Data Processor upon Data

Processor's request only where necessary to enable Data Processor to provide the Services.

2.1.5. Data Controller is responsible for independently determining whether the data security provided by Data Processor pursuant to the Agreement adequately meets Data Controller's obligations under applicable Data Protection Laws. Data Controller is also responsible for its secure use of Data Processor's services, including the obligation to securely backup or encrypt any such Personal Data.

2.2. Data Processor Covenants and Obligations

2.2.1. Data Processor warrants that no Applicable Privacy Law, or legal requirement, or privacy or information security enforcement action, investigation, litigation or claim, or any other circumstance, prohibits Data Processor from (i) fulfilling its obligations under this Addendum, or (ii) complying with instructions it receives from Data Controller concerning Personal Data.

2.2.2. In Processing Personal Data, Data Processor shall comply with (i) all Applicable Privacy Laws; (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security, including, without limitation, the Payment Card Industry Data Security Standard; and (iii) Data Controller's written instructions as set forth in the Agreement and this Addendum. Data Processor shall immediately inform Data Controller if, in Data Processor's opinion, an instruction from Data Controller infringes Applicable Privacy Laws.

2.2.3. Data Processor shall Process Personal Data only on behalf of and on documented instructions from Data Controller (including with regard to transfers of Personal Data), and only for the purposes of providing Services to Data Controller pursuant to the Agreement. Data Processor shall not take any other action involving Personal Data or carry out any other Processing, unless Data Processor is required or permitted to do so by applicable law to which Data Processor is subject. In such a case, Data Processor shall inform Data Controller of that legal requirement or basis before Processing the Personal Data, unless that law prohibits such information on important grounds of public interest.

2.2.4. Data Processor shall limit access to Personal Data to its Personnel who have a need to know the Personal Data as a condition to Data Processor's performance of services for or on behalf of Data Controller and who have and who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Data Processor shall exercise the necessary and appropriate supervision over its relevant Personnel to maintain appropriate privacy, confidentiality and security of

Personal Data. Data Processor shall ensure that Personnel with access to Personal Data are periodically trained regarding privacy and security.

2.2.5. In the event a privacy requirement, enforcement action, investigation, litigation, or claim, or any other circumstance, is reasonably likely to adversely affect Data Processor's ability to fulfill its obligations under this Addendum, Data Processor shall immediately inform Data Controller in writing and Data Controller may, in its sole discretion and without penalty of any kind to Data Controller, suspend the transfer or disclosure of Personal Data to Data Processor or access to Personal Data by Data Processor, terminate any further Processing of Personal Data by Data Processor, and terminate the Agreement and any related order(s), if doing so is necessary to comply with applicable Privacy Laws.

2.2.6. Data Processor shall develop, implement and maintain reasonable administrative, technical, physical, organizational and operational measures appropriate to the nature of the information to protect the Personal Data from unauthorized access, destruction, use, modification, or disclosure. Data Controller acknowledges that the security measures used by Data Processor are subject to technical progress and development and that Data Processor may update or modify such security measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of Personal Data.

2.2.7. Data Processor shall immediately, but in no event later than forty eight (48) hours after Data Processor's discovery of a Security Incident, notify Data Controller in writing of any Security Incident. Data Processor will promptly take all necessary and advisable corrective actions, and will cooperate fully with Data Controller in all reasonable and lawful efforts to prevent, mitigate or rectify such Security Incident.

2.3. **Data Subject and Regulator Requests**.

2.3.1. Data Processor shall immediately inform Data Controller in writing of any requests with respect to Personal Data received from Data Subjects. Data Controller shall be solely responsible for responding substantively to requests from Data Subjects regarding their Personal Data.

2.3.2. To the extent that Data Controller is not able to independently address a request from a Data Subject, then upon Data Controller's written request, Data Processor shall provide reasonable assistance to respond to requests from Data Subjects, subject to an additional fee. Data Processor will respond to such requests only in accordance with Data Controller's instructions.

2.3.3. Notwithstanding the foregoing, Data Processor shall have no obligation to reidentify or otherwise link information that is not maintained in a manner that would not be considered Personal Information. Further, notwithstanding anything in the contrary herein, Data Processor shall have no obligation to delete or return Personal Information where it is necessary for Data Processor to maintain the Personal Information in order to (a) complete the transaction for which the Personal Information was collected or otherwise perform a contract between Data Controller and a consumer; (b) detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity; (c) debug to identify and repair errors that impair existing intended functionality; (d) exercise a right under the law; (e) comply with applicable law or a legal obligation; and (f) otherwise use the Personal Information in a lawful manner that is compatible with the context in which the information was provided.

2.3.4. If Data Processor, either directly or indirectly, receives any communication from Regulators relating to Personal Data, Data Processor shall provide a copy to Data Controller within a commercially reasonable time, but no later than within five (5) business days. Data Processor shall not respond to any communication from a Regulator relating to Personal Data without the explicit written consent of Data Controller, unless required by law. Data Processor shall work in full cooperation with Data Controller on any permitted response(s) to Regulators without unreasonable delay.

2.3.5. If Data Processor is required by law to disclose Personal Data to law enforcement or government authorities, Data Processor shall notify Data Controller in writing and liaise with Data Controller before complying with such disclosure request, where allowed by law.

2.4. **Sub-Processors.**

2.4.1. Data Processor may engage Sub-Processors to Process Personal Data on Data Controller’s behalf, including to assist with hosting and infrastructure, to support product features and integrations, and for service and support. Data Processor’s current Sub-Processors are listed at https://drivecommerce.com/dpa-subprocessor. Data Controller authorizes the appointment of the Sub-Processors identified as of the effective date of this Addendum.

2.4.2. Data Processor may add or replace a Sub-Processor, provided that Data Processor provides Data Controller with at least 30 days’ advance notice of the intended addition or replacement of Sub-Processors giving Data Controller an opportunity to object to such changes, unless circumstances require a shorter notice period, in which case notice will be provided as soon as practicable. If the Data Controller sends Data Processor a written notice within 10 days of such notification setting forth a reasonable basis for objection related to data protection, the Parties will make a good-faith effort to resolve Data Controller’s objection. If Data Processor, in its discretion, requires use of the new or replacement Sub-Processor and is unable to satisfy Data Controller’s objection, either party may terminate the Agreement without liability to the other party (but without prejudice to any fees incurred by Data Controller prior to suspension or termination). If Data Controller does not provide a timely objection to any new or replacement Sub-Processor in accordance with this clause, Data Controller will be deemed to have consented to such Sub-Processor and waived its right to object.

2.4.3. Data Processor will impose data protection terms on Sub-Processors that provide at least the same level of protection for Personal Data as those in this Addendum, to the extent applicable to the nature of the services provided by such Sub-Processors. Data Processor will remain responsible for each Sub-Processor's compliance with the obligations of this Addendum and for any acts or omissions of such Sub-Processor that cause Data Processor to breach any of Data Processor's obligations under this Addendum.

2.5. **Demonstration of Compliance.** Data Processor shall make available to Data Controller all information necessary to demonstrate compliance with the obligations in this Addendum, upon reasonable request. Data Controller reserves the right to annually, or upon a Security Incident, or in relation to a Regulator's request, review and inspect Data Processor's information privacy and security policies, practices, and procedures, at Data Controller's sole cost. With reasonable prior notice, Data Controller or its authorized representatives reserve the right to inspect Data Controller information or materials in Data Processor's possession, custody or control, relating in any way to Data Processor's obligations, at Data Controller's sole cost. An inspection shall not unreasonably interfere with the normal conduct of Data Processor's business and Data Processor shall cooperate fully with any such inspection conducted by Data Controller or another auditor mandated by Data Controller, provided that Data Controller, its auditors, and other representatives shall first be contractually obligated to maintain the confidentiality of Data Processor's system, policies, practices and procedures.

2.6. **Deletion.** Data Processor shall delete or return Personal Data Processed pursuant to this Addendum upon the expiration or earlier termination of the Agreement, or such earlier time as Data Controller requests. In the event applicable law does not permit Data Processor to comply with the delivery or deletion of the Personal Data, Data Processor shall ensure the privacy, confidentiality and security of the Personal Data.

3. LIMITATION OF LIABILITY

Data Processor shall have no liability to Data Controller for losses, damages or costs that are indirect, special, punitive or consequential. Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this Addendum and the Standard Contractual Clauses, where applicable, whether in contract, tort or under any other theory of liability, is limited to a sum equal to the total amounts paid or payable for the services in the twelve-month period preceding the event giving rise to a claim. Data Processor disclaims all liability with respect to third-party products that Data Controller may use.

4. Additional Provisions for Regulated United States Data:

4.1. When processing Personal Data subject to United States Data Protection Laws, the terms “**Business**,” “**Sells**,” “**Service Provider**”, “**Third Party**”, “**Deidentify**”, and “**Aggregate**” shall have the meaning ascribed to them in such applicable laws.

4.2. Data Processor’s security measures shall ensure a level of security appropriate to the risk, taking into account controls identified in applicable United States Data Protection Laws, for example, the 20 controls listed in the Center for Internet Security’s Critical Security Controls and the guidelines in the California Attorney General’s 2016 Data Breach Report as to California Personal Data.

4.3. Data Processor shall not Sell Personal Data or share or transfer it to any Third Party in exchange for any monetary or other valuable consideration.

4.4. Data Controller has the right to take reasonable and appropriate steps to help ensure that Data Processor uses Personal Data in a manner consistent with Data Controller’s obligations under applicable United States Data Protection Laws, and further has the right upon notice to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of Personal Data.

5. Additional Provisions for European Data:

5.1. Data Controller acknowledges that Data Processor is in the United States. To the extent that Data Processor receives Personal Data relating to Data Subjects in Europe, Data Processor shall provide an adequate level of privacy protection for such Personal Data (e.g., by providing at least the same level of privacy protection as is required by a data transfer agreement based on the Standard Contractual Clauses (EU Controller to non-EU Processor) adopted by the EU Commission (“**Data Transfer Agreement**”)). The Parties will enter into any further written agreements as are necessary (in Data Controller’s reasonable determination) to comply with Applicable Privacy Laws, including with respect to any cross-border data transfer of Personal Data, whether to or from Data Processor.

5.2. To the extent that Data Processor has information reasonably available to it, and Data Controller does not otherwise have access to the required information, Data Processor will provide reasonable assistance to Data Controller with any data protection impact assessments, and prior consultations with supervisory authorities to the extent required by Applicable Laws.

6. MISCELLANEOUS

6.1. Any provision of this Addendum that is prohibited or unenforceable shall be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this Addendum.

6.2. Except as provided below, notices provided hereunder must be in writing and sent by e-mail, facsimile or certified mail, return receipt requested. Notices to Data Processor shall be sent to Drive Commerce, 500 Westover Dr #31793, Sanford, NC 27330; mark@drivecommerce.com; Attention: Mark Barnum. .

6.3. This Addendum shall end automatically when the Agreement expires or is terminated. In the case of any non-compliance by Data Processor with any of the obligations under this Addendum, or the Applicable Privacy Laws, Data Controller may, by giving written notice, immediately terminate the Agreement, suspend any Personal Data transmission under the Agreement, or require Data Processor to cease or suspend any or all processing of Personal Data. Termination or expiration of this Addendum shall not discharge Data Processor from its obligations meant to survive the termination or expiration of this Addendum, provided that if termination of this Addendum requires Data Processor to modify the services provided pursuant to the Agreement, the parties shall enter into a mutually-acceptable amendment of the Agreement or any related statement of work.

6.4. This Addendum is binding upon successors and assigns of the parties.

6.5. A waiver by either party of any term or condition of the Addendum in one or more instances shall not constitute a permanent waiver of the term or condition or any other term or condition of the Addendum or a general waiver.

6.6. As required or on request, Data Processor agrees that Data Controller may provide a summary or copy of this Addendum to any government agency.

6.7. This Addendum will be governed by and construed in accordance with Michigan law, unless required otherwise by Applicable Privacy Laws or as otherwise specified in the Parties' Agreement. The Parties consent to the personal jurisdiction of, and venue in, Michigan, unless another court is specified in the Agreement.

6.8. To the extent required to comply with Applicable Privacy Laws, or the requirements of a competent supervisory authority, Data Processor may update this Addendum at this URL from time to time by posting an updated DPA at this URL and providing notice to Data Controller. Should Data Controller object to the amended terms, it shall communicate such objections to Data Processor in writing within 10 days after delivery of such notice. Continued performance of the Agreement constitutes Data Controller’s acceptance of the updated Addendum.