MAXIMOR AI DATA PROCESSING ADDENDUM

This Data Processing Addendum (including all Schedules attached hereto, the "**DPA**") is incorporated into, and is subject to the terms and conditions of, the Customer Agreement or other written or electronic agreement ("**Agreement**") between Prosperous Commerce, Inc. d/b/a Maximor AI ("**Maximor AI**") and the entity identified as "Customer" in the Agreement ("**Customer**"). This DPA applies to the extent Maximor AI's Processing of Customer Personal Data is subject to the Data Protection Laws. This DPA shall be effective for the term of the Agreement.

1. Definitions

1.1. For the purposes of this DPA:

1.1.1. "**Customer Personal Data**" means the Personal Data described under Schedule 1 to this DPA;

1.1.2. "**Data Protection Laws**" means all laws relating to data protection and privacy applicable to Maximor AI's Processing of Customer Personal Data in any jurisdiction where Customer and/or Maximor AI operates, including without limitation, European Data Protection Law and the laws and regulations of the United States and its states, as amended from time to time, to the extent applicable to the relevant party;

1.1.3. "**Data Subjects**" means the individuals identified in Schedule 1;

1.1.4. "**European Data Protection Law**" means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and all other privacy and data protection laws of the European Economic Area ("**EEA**"), and their respective Member States, Switzerland and the United Kingdom ("**UK**"), including without limitation the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) (the "**UK GDPR**"), and all laws implementing or supplementing the foregoing.

1.1.5. "**Personal Data**" means any information that reasonably relates, directly or indirectly, to an identified or identifiable Data Subject;

1.1.6. "**Processing**" (including its cognate "**Process**") means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.1.7. "**Security Incident**" means a material breach of security leading to the unauthorized or unlawful access by a third party, or confirmed accidental or unlawful destruction, loss or alteration, of Customer Personal Data; and

1.1.8. **"Standard Contractual Clauses**" means (i) Module 2 of the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj (the "**EU SCCs**").

1.1.9. "**UK Addendum**" means the International Data Transfer Addendum to the Standard Contractual Clauses issued by the UK Information Commissioner's Office, in force as of 21 March 2022, available at international-data-transfer-addendum.pdf (ico.org.uk).

1.2. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

2. Processing of Customer Personal Data

2.1. Maximor AI will Process Customer Personal Data on behalf of Customer and in accordance with Customer's prior written instructions, including any instructions provided through Customer's use of the Service. Maximor AI is hereby instructed to Process Customer Personal Data to the extent necessary to provide the Service as set forth in the Agreement and this DPA and in accordance with Data Protection Laws.

2.2. Maximor AI will inform Customer if, in its opinion, an instruction from Customer infringes the Data Protection Laws, unless it is prohibited from doing so by law on important grounds of public interest.

2.3. The details of Maximor AI's Processing of Customer Personal Data are described in Schedule 1.

2.4. If applicable laws preclude Maximor AI from complying with Customer's instructions, Maximor AI will inform Customer of its inability to comply with the instructions, to the extent permitted by law.

2.5. Each of Customer and Maximor AI will comply with their respective obligations under the Data Protection Laws.

2.6. Maximor AI certifies that it will not (a) "sell" (as defined in Data Protection Laws) Customer Personal Data; (b) share or otherwise disclose Customer Personal Data to third parties for targeted advertising purposes; (c) retain, use, or disclose Customer Personal Data for any purpose other than as permitted under this DPA and in accordance with the Agreement; or (d) retain, use, or disclose Customer Personal Data other than in the context of the direct relationship with Customer in accordance with the Agreement and Data Protection Laws.

3. Restricted Data Transfers

3.1. In the event that Customer is subject to European Data Protection Law and the transfer of Customer Personal Data to Maximor AI would be restricted in the absence of the Standard Contractual Clauses, the parties agree that the Standard Contractual Clauses shall be incorporated into this DPA with Customer as the "data exporter" and Maximor AI as the "data importer."

3.2. For purposes of the EU SCCs the parties agree that:

3.2.1. In Clause 7, the optional docking clause will not apply;

3.2.2. In Clause 9, Option 2 will apply and the time period for prior notice of Subprocessor changes will be as set forth in Section 5.1 of this DPA;

3.2.3. In Clause 11, the optional language will not apply;

3.2.4. For the purpose of Clause 17, the EU SCCs shall be governed by the laws of Ireland;

3.2.5. For the purpose of Clause 18(b), the parties agree to submit to the jurisdiction of the courts of Ireland;

3.2.6. For Annex I, Section A (List of Parties), (i) the data exporter's and the data importer's identity and contact details and, where applicable, information about their respective data protection officer and/or representative in the EEA are those set forth in the Agreement or as otherwise communicated by each party to the other party; (ii) Customer is a controller, and Maximor AI is a processor; (iii) the activities relevant to the data transferred under the EU SCCs relate to the provision of the Services pursuant to the Agreement; and (iv) entering into this DPA shall be treated as each party's signature of Annex I, Section A, as of the effective date of this DPA;

3.2.7. For Annex I, Section B (Description of Transfer): (i) Schedule 1 to this DPA describes Maximor AI's Processing of Customer Personal Data; (ii) the frequency of the transfer is continuous (for as long as Customer uses the Services); (iii) Customer Personal Data will be retained in accordance with Clause 8.5 of the EU SCCs and this DPA; (iv) Maximor AI uses Subprocessors to support the provision of the Services.

3.2.8. For Annex I, Section C (Competent Supervisory Authority), the competent supervisory authority identified in accordance with Clause 13 of the EU SCCs is the competent supervisory authority communicated by Customer to Maximor AI. Unless and until Customer communicates a competent supervisory authority to Maximor AI, the competent supervisory authority shall be the Irish Data Protection Commission.

3.2.9. For the purposes of Annex II, data importer has implemented and will maintain appropriate technical and organizational measures to protect the security, confidentiality and integrity of Customer Personal Data as described in Schedule 2.

3.3. For the purposes of the UK Addendum parties agree that Part 1, tables 1, 2 and 3 of the UK SCCs will be deemed to be completed like the equivalent provisions in the EU SCCs. For the purpose of Part 1, Table 4, the party that may end the UK Addendum in accordance with Section 19 of the UK Addendum is the importer.

4. Confidentiality and Security

4.1. Maximor AI will require Maximor AI's personnel who access Customer Personal Data to commit to protect the confidentiality of Customer Personal Data.

4.2. Maximor AI will implement commercially reasonable technical and organisational measures, as further described in Schedule 2, that are designed to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

4.3. To the extent required by Data Protection Laws, Maximor AI will provide Customer with reasonable assistance as necessary for the fulfilment of Customer's obligations under Data Protection Laws to maintain the security of Customer Personal Data.

5. Subprocessing

5.1. Customer agrees that Maximor AI may use the third-party suppliers listed in Schedule 3 to Process Customer Personal Data on its behalf for the provision of the Services under the Agreement (each a "**Subprocessor**"). Maximor AI will inform Customer of any intended changes concerning the addition or replacement of Subprocessors and Customer will have an opportunity to object to such changes on reasonable grounds within seven days after being notified. In response to Customer's reasonable objection, the parties will work together in good faith to determine an appropriate resolution.

5.2. Maximor AI will be liable to Customer for breaches of this DPA caused by its Subprocessors' acts and omissions as it would be for its own.

6. Data Subject Rights

Customer is responsible for responding to any Data Subject requests relating to Customer Personal Data ("**Requests**"). If Maximor AI receives any Requests during the term, Maximor AI will advise the Data Subject to submit the request directly to Customer. Maximor AI will provide Customer with self-service functionality or other reasonable assistance to permit Customer to respond to Requests.

7. Security Incidents

Upon becoming aware of a Security Incident affecting Customer Personal Data, Maximor AI will (i) promptly take measures designed to remediate the Security Incident and (ii) notify Customer without undue delay. Customer is solely responsible for complying with Security Incident notification requirements applicable to Customer. At Customer's request, Maximor AI will reasonably assist Customer's efforts to notify Security Incidents to the competent data protection authorities and/or affected Data Subjects, if Customer is required to do so under the Data Protection Laws. Maximor AI's notice of or response to a Security Incident under this Section 7 will not be an acknowledgement or admission by Maximor AI of any fault or liability with respect to the Security Incident.

8. Data Protection Impact Assessment; Prior Consultation

Taking into account the nature of the Processing and the information available to Maximor AI, Maximor AI will reasonably assist Customer in conducting data protection impact assessments and consultation with data protection authorities if Customer is required to engage in such activities under applicable Data Protection Laws and such assistance is necessary and relates to the Processing by Maximor AI of Customer Personal Data.

9. Deletion of Customer Personal Data

Customer instructs Maximor AI to delete Customer Personal Data within 90 days of the termination of the Agreement and delete existing copies unless applicable law requires otherwise. The parties agree that the certification of deletion described in Clause 8.5 of the EU SCCs and Clause 12 of the UK SCCs, if applicable, shall be provided only upon Customer's written request. Notwithstanding the foregoing, Maximor AI may retain Customer Personal Data to the extent and for the period required by applicable laws provided that Maximor AI maintains the confidentiality of all such Customer Personal Data and Processes such Customer Personal Data only as necessary for the purpose(s) specified in the applicable laws requiring its storage.

10. Audits

10.1. Customer may audit Maximor AI's compliance with its obligations under this DPA up to once per year. In addition, Customer may perform more frequent audits (including inspections) in the event: (1) Maximor AI suffers a Security Incident affecting Customer Personal Data; (2) Customer has genuine, documented concerns regarding Maximor AI's compliance with this DPA or the Data Protection Laws; or (3) where required by the Data Protection Laws, including where mandated by regulatory or governmental authorities with jurisdiction over Customer Personal Data. Maximor AI will contribute to such audits by providing Customer or Customer's regulatory or governmental authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Service, as described below.

10.2. To request an audit, Customer must submit a detailed proposed audit plan to support@maximor.ai at least one month in advance of the proposed audit start date. The proposed audit plan must describe the proposed scope, duration, start date of the audit, and the

identity of any third party Customer intends to appoint to perform the audit. Maximor AI will review the proposed audit plan and provide Customer with any concerns or questions (for example, Maximor AI may object to the third party auditor as described in Section 10.3, provide an Audit Report as described in Section 10.4, or identify any requests for information that could compromise Maximor AI confidentiality obligations or security, privacy, employment or other relevant policies). The parties will negotiate in good faith to agree on a final audit plan at least two weeks in advance of the proposed audit start date. Nothing in this Section 10 shall require Maximor AI to breach any duties of confidentiality.

10.3. Maximor AI may object to third party auditors that are, in Maximor AI's reasonable opinion, not suitably qualified or independent, a competitor of Maximor AI, or otherwise manifestly unsuitable. Customer will appoint another auditor or conduct the audit itself if the parties cannot resolve the objection after negotiating in good faith.

10.4. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor on Maximor AI's systems that Process Customer Personal Data ("Audit Reports") within twelve (12) months of Customer's audit request and Maximor AI confirms there are no known material changes in the controls audited, Customer agrees to accept the Audit Report in lieu of requesting an audit of the controls covered by the Audit Report.

10.5. The audit must be conducted at a mutually agreeable time during regular business hours at the applicable facility, subject to the agreed final audit plan and Maximor AI's health and safety or other relevant policies and may not unreasonably interfere with Maximor AI business activities.

10.6. Any audits are at Customer's expense and Customer will promptly disclose to Maximor AI any perceived non-compliance or security concerns discovered during the audit, together with all relevant details.

10.7. The parties agree that the audits described in Clause 8.9 of the EU SCCs and Clause 5(f) of the UK SCCs, if applicable, shall be performed in accordance with this Section 10.

11. Analytics Data

Customer acknowledges and agrees that Maximor AI may create and derive from Processing related to the Service anonymized and/or aggregated data that does not identify or relate to Customer or any Data Subject ("**Analytics Data**"), and use, publicize or share with third parties such Analytics Data to improve the Service and for Maximor AI's other legitimate business purposes in accordance with Data Protection Laws.

12. Liability

12.1. Each party's liability towards the other party under or in connection with this DPA will be limited in accordance with the provisions of the Agreement.

12.2. Customer acknowledges that Maximor AI is reliant on Customer for direction as to the extent to which Maximor AI is entitled to Process Customer Personal Data on behalf of Customer in performance of the Service. Consequently, Maximor AI will not be liable under the Agreement for any claim brought by a Data Subject arising from (a) any action or omission by Maximor AI in compliance with Customer's instructions or (b) from Customer's failure to comply with its obligations under the Data Protection Laws.

13. General Provisions

With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail. In the event of

inconsistencies between the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

SCHEDULE 1

Details of Processing

1. **Categories of Data Subjects**. This DPA applies to Maximor AI's Processing of Customer Personal Data relating to Customer's employees, contractors, clients/consumers, and other authorized users of the Service ("Data Subjects").

2. **Types of Personal Data**. The extent of Customer Personal Data Processed by Maximor AI is determined and controlled by Customer in its sole discretion and includes user ID, passwords, and any other Personal Data that may be transmitted through the Service by Data Subjects.

3. **Subject-Matter and Nature of the Processing**. Customer Personal Data will be subject to the Processing activities that Maximor AI needs to perform in order to provide the Service pursuant to the Agreement.

4. **Purpose of the Processing**. Maximor AI will Process Customer Personal Data for purposes of providing the Service as set out in the Agreement.

5. **Duration of the Processing**. Customer Personal Data will be Processed for the duration of the Agreement, subject to Section 9 of the DPA.

SCHEDULE 2

Security Measures

Maximor AI will implement and maintain the security practices and procedures set out in this Schedule 2.

1. Organizational management and staff responsible for the development, implementation and maintenance of Maximor AI's information security program.

2. Periodic review and assessment of risks to Maximor AI's organization, monitoring and maintaining compliance with Maximor AI's policies and procedures, and reporting the condition of its information security and compliance to internal senior management as appropriate.

3. Data security controls which include logical segregation of data, restricted (e.g., role-based) access and monitoring, and use of commercially available and industry standard encryption technologies for Customer Personal Data as appropriate.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength and password management requirements for assigned Maximor AI credentials as appropriate.

6. Change management procedures and tracking mechanisms designed to test, approve and monitor changes to Maximor AI's technology and information assets.

7. Incident response procedures design to allow Maximor AI to investigate, respond to, mitigate and notify events related to Maximor AI's technology and information assets.

8. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack, as appropriate.

9. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.