DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT (the "Agreement") is made and entered by and between:

GAMMA TECHNOLOGIES, LLC, a Delaware limited liability company, with its principal place of business at 700 Oakmont Lane, Suite 300, Westmont, IL 60559 USA on its own behalf and for its wholly owned affiliates (the "Controller");

and

PROCESSOR: a company engaged by Controller who, by the nature of the engagement, will process personal data on behalf of Controller (the “Processor”).

RECITALS

WHEREAS, the Controller is a U.S. software company with multiple global offices, including but not limited to in the European Union, and is subject to the requirements of the General Data Protection Regulation (EU) 2016/679 ("EU GDPR"), the United Kingdom General Data Protection Regulation (the "UK GDPR"), and other applicable data protection laws;

WHEREAS, the Controller engages the Processor to provide services that involve the processing of personal data on behalf of the Controller;

WHEREAS, the Parties wish to enter into this Agreement to ensure compliance with the applicable data protection laws, including the EU GDPR, UK GDPR, and jurisdiction-specific regulations, and to set forth the terms and conditions under which the Processor shall process personal data, including any special categories of personal data, on behalf of the Controller;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. DEFINITIONS

1.1 Capitalized terms used but not defined in this Agreement shall have the meanings given to them in the applicable Data Protection Laws.

1.2 "Data Protection Laws" means:
(a) the EU GDPR, and any applicable national laws implementing the EU GDPR;
(b) the UK GDPR and the Data Protection Act 2018;
(c) the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), as applicable;
(d) any other applicable laws and regulations relating to the processing of personal data and privacy, including but not limited to the Federal Trade Commission Act, the Children's Online Privacy Protection Act (COPPA), and state-specific data protection laws such as the New York SHIELD Act and the Virginia Consumer Data Protection Act (VCDPA).

1.3 "Personal Data" means any information relating to an identified or identifiable natural person that is processed by the Processor on behalf of the Controller pursuant to this Agreement, including any special categories of personal data.

1.4 "Processing" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.5 "Sub-Processor" means any processor engaged by the Processor to assist in fulfilling its obligations under this Agreement.

1.6 "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as adopted by the European Commission, or any successor clauses adopted to replace them.

2. SUBJECT MATTER AND DURATION OF THE PROCESSING

2.1 The subject matter of the Processing is the provision of goods/services by the Processor.

2.2 The duration of the Processing shall be for the term of the relationship between the Parties, unless otherwise agreed in writing.

3. CONTROLLER'S INSTRUCTIONS AND PROCESSOR'S COMPLIANCE

3.1 The Processor shall only Process the Personal Data in accordance with the Controller's documented instructions, unless required to do so by applicable Data Protection Laws, in which case the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.2 The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction from the Controller infringes the Data Protection Laws.

3.3 The Processor shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.4 The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing the information required under Article 30(2) of the GDPR and make it available to the Controller upon request.

4. SECURITY OF PROCESSING

4.1 The Processor shall implement and maintain the following technical and organizational measures to ensure a level of security appropriate to the risk of the Processing:

(a) Pseudonymization and encryption of Personal Data during transmission and at rest;
(b) Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
(c) Measures to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
(d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
(e) Access controls and authentication mechanisms to ensure that only authorized personnel have access to Personal Data;
(f) Network security measures, including firewalls, intrusion detection and prevention systems, and regular vulnerability scans;
(g) Physical security measures for data centers and offices where Personal Data is processed;
(h) Regular employee training on data protection and information security best practices;
(i) Incident response and management procedures;
(j) Data minimization and retention policies to ensure that only necessary Personal Data is collected and processed;

4.2 In assessing the appropriate level of security, the Processor shall take 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.

4.3 The Processor shall conduct regular risk assessments to identify and mitigate potential threats to the security of Personal Data and shall promptly implement any additional security measures recommended as a result of such assessments.

5. USE OF SUB-PROCESSORS

5.1 The Processor shall not engage any Sub-Processor without the prior written authorization of the Controller. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-Processors, thereby giving the Controller the opportunity to object to such changes.

5.2 Where the Processor engages a Sub-Processor to carry out specific Processing activities on behalf of the Controller, the Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those set out in this Agreement, including but not limited to the implementation of appropriate technical and organizational measures.

5.3 The Processor shall remain fully liable to the Controller for the performance of the Sub-Processor's obligations.

5.4 The Processor shall maintain an up-to-date list of all Sub-Processors engaged in the Processing of Personal Data under this Agreement and shall make this list available to the Controller upon request.

6. DATA SUBJECT RIGHTS

6.1 The Processor shall assist the Controller, by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller's obligations to respond to requests from data subjects exercising their rights under the applicable Data Protection Laws, including but not limited to:

(a) The right of access;
(b) The right to rectification;
(c) The right to erasure ('right to be forgotten');
(d) The right to restriction of processing;
(e) The right to data portability;
(f) The right to object to processing;
(g) The right not to be subject to automated individual decision-making, including profiling.

6.2 The Processor shall promptly notify the Controller of any communication from a data subject regarding the Processing of their Personal Data, without responding to the data subject unless authorized to do so by the Controller.

6.3 The Processor shall provide the Controller with all necessary information and assistance to enable the Controller to respond to data subject requests within the timeframes specified by the applicable Data Protection Laws.

6.4 In the event that a data subject request requires the Processor to take specific actions (e.g., providing a copy of Personal Data, deleting Personal Data), the Processor shall do so promptly and in accordance with the Controller's instructions.

7. PERSONAL DATA BREACHES

7.1 The Processor shall notify the Controller without undue delay, and in any event within 24 hours, after becoming aware of a Personal Data Breach affecting the Personal Data processed under this Agreement.

7.2 The notification shall include, at a minimum, the following information:
(a) A description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned;
(b) The name and contact details of the data protection officer or other contact point where more

information can be obtained;
(c) A description of the likely consequences of the Personal Data Breach;
(d) A description of the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.3 The Processor shall cooperate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

7.4 The Processor shall maintain a record of all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects, and the remedial action taken.

8. AUDIT AND INSPECTION

8.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this Agreement and the Data Protection Laws.

8.2 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, and provide access to any premises, systems, or documents relevant to the Processing of the Personal Data.

8.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction from the Controller infringes the Data Protection Laws.

8.4 The Processor shall designate a point of contact for all audit-related matters and shall cooperate fully with the Controller or its designated auditor throughout the audit process.

9. DELETION OR RETURN OF PERSONAL DATA

9.1 Upon the termination of the provision of the services relating to the Processing, the Processor shall, at the choice of the Controller, delete or return all the Personal Data to the Controller and delete any existing copies, unless applicable Data Protection Laws require the Processor to store the Personal Data.

9.2 The Processor shall provide the Controller with a written confirmation of the deletion or return of the Personal Data within five (5) business days of the termination of the services.

9.3 In the event that the Processor is required by applicable Data Protection Laws to retain any Personal Data beyond the termination of services, the Processor shall inform the Controller of such requirement and shall ensure that the retained Personal Data is protected in accordance with this Agreement for as long as it is retained.

10. INTERNATIONAL DATA TRANSFERS

10.1 The Processor shall not transfer or disclose any Personal Data to any third country or international organization, unless authorized in writing by the Controller.

10.2 Where the Controller authorizes an international transfer of Personal Data, the Parties shall comply with the requirements of the applicable Data Protection Laws, including, where necessary, entering into Standard Contractual Clauses or implementing other appropriate transfer mechanisms.

10.3 The Processor acknowledges that transfers of Personal Data from the EU/EEA to the United States are subject to additional scrutiny following the Schrems II decision. The Processor shall:

(a) Implement supplementary measures as necessary to ensure an essentially equivalent level of protection for the Personal Data as guaranteed within the EU/EEA;
(b) Promptly inform the Controller of any inability to comply with the Standard Contractual Clauses or other transfer mechanisms;
(c) Assist the Controller in conducting transfer impact assessments and implementing any additional safeguards required to legitimize the transfer of Personal Data.

10.4 In the event of any changes to the legal framework governing international data transfers, including but not limited to changes in the adequacy status of any country or the adoption of new transfer mechanisms, the Parties agree to promptly review and, if necessary, update this Agreement to ensure continued compliance with Data Protection Laws.

11. LIABILITY AND INDEMNIFICATION

11.1 The Processor shall indemnify and hold the Controller harmless from and against any and all claims, liabilities, costs, and expenses (including reasonable legal fees) resulting from the Processor's breach of this Agreement or the applicable Data Protection Laws.

11.2 The Parties' liability in relation to this Agreement shall be subject to the limitations of liability set out in any contractual document executed by the Parties, provided that such limitations shall not apply to liability arising from breaches of data protection obligations under this Agreement or applicable Data Protection Laws.

11.3 Each Party shall maintain appropriate insurance coverage to cover its potential liabilities under this Agreement and shall provide evidence of such coverage upon request.

12. TERM AND TERMINATION

12.1 This Agreement shall commence on the Effective Date and shall continue in full force and effect for the duration of the relationship between the Parties, unless terminated earlier in accordance with the terms of this Agreement or any applicable master agreement executed by the

Parties.

12.2 The Controller may terminate this Agreement immediately if the Processor is in material breach of any of its obligations under this Agreement or the applicable Data Protection Laws.

12.3 Upon termination of this Agreement for any reason, the Processor shall cease all Processing of Personal Data on behalf of the Controller, except as may be required by applicable Data Protection Laws.

13. MISCELLANEOUS

13.1 This Agreement shall be governed by and construed in accordance with the laws of the State of Illinois, USA, without regard to its conflict of law provisions.

13.2 Any dispute arising out of or in connection with this Agreement shall be resolved by the courts of the State of Illinois, USA, which shall have exclusive jurisdiction.

13.3 This Agreement may only be modified or amended by a written instrument signed by both Parties.

13.4 If any provision of this Agreement is held to be invalid or unenforceable, the remainder of the Agreement shall continue in full force and effect.

13.5 This Agreement constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior agreements, understandings, and communications, whether written or oral, between the Parties regarding such subject matter.

13.6 The Parties acknowledge the potential implications of Article 71 of the EU-UK Withdrawal Agreement and the "Frozen GDPR" regime. In the event of any changes to the UK's data protection landscape, including but not limited to the loss of adequacy status, the Parties agree to promptly review and amend this Agreement as necessary to ensure continued compliance with applicable Data Protection Laws.

13.7 The Parties shall review this Agreement annually, or more frequently if required by changes in applicable Data Protection Laws or the nature of the Processing activities, to ensure its continued adequacy and effectiveness.

13.8 Nothing in this Agreement shall be construed to create a joint venture, partnership, or agency relationship between the Parties.

13.9 The failure of either Party to enforce any right or provision in this Agreement shall not constitute a waiver of such right or provision unless acknowledged and agreed to by such Party in writing.

13.10 This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.