DATA PROCESSING ADDENDUM

For purposes of this Data Processing Addendum ("DPA") and all related activity, the term "Service Provider" means the entity identified as the Seller, Vendor, Contractor, Service Provider, Supplier, or similar on the applicable master services agreement, statement of work, purchase order, supply agreement (regardless of how titled) entered into by Company and Service Provider ("Agreement"), and the term "Company" means the company(ies) identified as the purchaser in the applicable Agreement. The DPA will be deemed accepted by Service Provider upon the first of the following to occur: (i) Service provider communicating to Company its acceptance of the same; (ii) any performance by Service Provider under the Agreement; or (iii) any other conduct that recognizes the existence of a contract with respect to the subject matter of the Agreement. Unless otherwise set forth in this DPA, Service Provider shall, at its own cost and expense, meet and exceed the standards, and satisfy its responsibilities, set forth herein. In the event of conflict between this DPA and the Agreement, the terms and conditions set forth in the DPA shall supersede and control. For the avoidance of doubt, any terms or conditions of the Agreement not otherwise addressed herein shall remain in full force and effect.

1. Definitions

(a) "**Applicable Data Protection Law**" means all data protection laws, regulations, or statutes applicable to the Agreement, including the California Consumer Privacy Act and the European Union ("EU"), General Data Protection Regulation ("**GDPR**") and its implementing laws of the EU Member States and Retained Regulation (EU) 2016/679 **("UK GDPR")** and its implementing legislation the Data Protection Act 2018.

(b) "**Company Data"** means any Confidential Information of Company to which Service Provider has been given access, custody, or control.

(c) "**Confidential Information**" means information that, under the circumstances in which it is disclosed or accessed, a reasonable person would recognize it as being a trade secret, or confidential or proprietary in nature. Confidential Information includes any and all Personal Data.

(d) "**Personal Data**" means any information, in any form or format, that Company provides Service Provider, or to which Company grants Service Provider access, that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, and that is subject to, or otherwise afforded protection under, an Applicable Data Protection Law.

(e) "**Process**" means any operation, or set of operations, which is, or that are, performed on Company Data, whether or not by automated means, such as collecting, recording, organizing, structuring, storing, altering, retrieving, intercepting, using, disclosing, disseminating, combining, restricting, erasing, destroying, or disposing of, Company Data.

(f) "**Security Breach**" means any actual or reasonably suspected compromise of the security, confidentiality, or integrity of Company Data, or to the physical, technical, or administrative measures implemented by Service Provider to protect or safeguard Company Data. A "Security Breach" includes the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Company Data.

2. Data Processing

(a) The parties hereby acknowledge and agree that as between Company and Service Provider, Company, alone or jointly with others, determines the means and purposes of the Processing of Company Data and Service Provider Processes Company Data on behalf of Company. The subject matter and type of Company Data, and the nature and purpose of Processing Company Data is specified in the Agreement(s) and such Agreement(s) represent(s) the documented instructions of Company. Service Provider shall only Process Company Data in accordance with all Applicable Data Protection Law, and to the minimal extent necessary and as required to perform its obligations under the Agreement, unless otherwise required by law. In the event Service Provider is compelled by law to Process Company Data beyond, or in contrast to, the terms and conditions in the Agreement or this DPA, Service Provider shall notify Company of the same prior to such Processing, unless such notification is expressly prohibited by law. Service Provider shall, promptly and without delay, notify Company if Company's document instructions infringe any Applicable Data Protection Law.

(b) Without limiting Section 2(a) of this DPA, Service Provider shall not, unless otherwise approved in writing by Company (i) retain, use, or disclose Company Data for any purpose other than for the specific purpose of performing the services specified in this Agreement or as permitted by Applicable Data Protection Law, including retaining, using, or disclosing Company Data for a commercial purpose other than providing the services specified in the Agreement, or (ii) collect, sell, or use Company Data, except as necessary to satisfy its obligations under the Agreement.

3. Confidentiality and Security

(a) Service Provider shall (i) maintain the confidentiality of all Company Data, and ensure that all individuals who are authorised to Process Company Data on its behalf have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, (ii) limit access to Company Data to only those individuals who have a business need for such access, and (iii) take reasonable steps to ensure the reliability of all individuals who have access to Company Data.

(b) Service Provider shall implement and maintain an information security program to protect Company Data from a Security Breach. Service Provider's information security program shall, at all times, meet or exceed (i) the standards set forth in ISO/IEC 27001:2013 (or any subsequent and superseding publication); (ii) any standards substantially similar to those set forth in Section 3(b)(i) of this DPA; or (iii) at a minimum, commercially reasonable industry standards. Without limiting the foregoing, Service Provider's information security program shall, as appropriate, include network and system security monitoring, authentication and access controls, and encryption protocols designed to protect Company Data.

(c) Service Provider shall, periodically and from time to time, have a third-party audit firm or consultant conduct a risk assessment, penetration test, and network-level vulnerability scan of Service Provider's information security program, and its information technology systems, networks, and environment, as appropriate.

4. Cooperation and Assistance

(a) Service Provider shall provide reasonable assistance to Company to enable Company to comply with its obligations and responsibilities under any Applicable Data Protection Law, including consultations with regulatory authorities, executing data protection impact assessments, and responding to individuals exercising their data privacy rights.

(b) Service Provider shall, immediately and without delay, refer to Company any correspondence, inquiry, complaint, request, or demand (collectively, or individually, "Data Notice") concerning the Processing of Company Data and shall not respond to any such Data Notice, unless otherwise required by law. Upon written request from Company, and without limiting Section 4(a) of this DPA Service Provider shall promptly (i) provide Company access to Company Data in Service Provider's custody or control, or in the custody or control of a third-party acting on behalf of Service Provider, and (ii) amend, correct, delete, or cease, or restrict the use of, Company Data.

(c) Service Provider shall, within ten (10) business days after termination of any Agreement and at Company's discretion, return all Company Data and all copies thereof, or destroy and certify the destruction of the same, unless such return or destruction is prohibited by law. Notwithstanding the foregoing, Service Provider may destroy Company Data that is stored in a back-up or archived format in accordance with its normal retention schedule so long as such Company Data is otherwise retained in accordance with this DPA.

5. Audits. Upon written request from Company, Service Provider shall promptly make available to Company any and all information necessary to demonstrate compliance with its obligations set forth in this DPA. Notwithstanding the foregoing, Service Provider shall submit to audits conducted by Company, or a third-party on Company's behalf, to demonstrate compliance with its obligations under this DPA so long as Company provides Service Provider at least thirty (30) days advanced written notice and the audit is performed during the normal business hours of Service Provider and does not materially interfere with Service Provider's business operations. Company shall be responsible for all costs and expenses directly related to an audit undertaken pursuant to this Section.

6. Security Breach Procedures

(a) Service Provider shall immediately notify Company of a Security Breach involving Company Data in Service Provider's custody or control, or in the custody or control of a third-party acting on behalf of Service Provider. Service Provider shall, to the greatest extent possible, include in the foregoing notification to Company the following: (i) a description of the nature of the Security Breach, including (where possible) the categories and approximate number of individuals likely to be impacted by the Security Breach; (ii) a description of the likely consequences caused by the Security Breach; (iii) a description of the measures taken, or proposed to be taken, to address the Security Breach; and, (iv) contact information of a Service Provider representative from whom more information about the Security Breach can be obtained.

(b) Service Provider shall immediately contain, mitigate, and remedy a Security Breach. Service Provider shall reimburse Company for all actual costs incurred by Company in responding to, and mitigating damages caused by, a Security Breach involving Company Data in Service Provider's custody or control, or in the custody or control of a third-party acting on the behalf of Service Provider. In the event of any Security Breach, Service Provider shall, immediately and without delay, assess its information security program and use its best efforts to remediate any deficiencies therein.

7. Third-Party Subcontracting

(a) Unless otherwise prohibited or restricted by the Agreement, Company acknowledges and agrees that Service Provider may authorize a subcontractor to assist with satisfying the terms and conditions of the Agreement, including its Processing activities therein; provided however, Service Provider executes a written agreement with any such subcontractor that is the same as, or substantially similar to, the terms and conditions set forth herein and Service Provider remains liable to Company for any and all breaches or violations of this DPA caused by any such subcontractor.

(b) Service Provider shall, immediately upon execution of this DPA and at least once a year thereafter, provide written notice to Company of any subcontractor involved in the Processing of Company Data. Service Provider further agrees to provide at least fifteen (15) days advanced notice to Company of any intended changes concerning the addition or replacement of any such subcontractor thereby providing Company the opportunity to object to such change. The parties shall, in good faith, seek to resolve any objections, issues, or disputes concerning Service Provider's use, or proposed use, of a subcontractor.

8. Data Localisation and Transfers

(a) Unless otherwise agreed to in writing by Company, Service Provider shall maintain, and ensure all subcontractors maintain, Company Data within the jurisdictions in which Company and/or Service Provider are located. In the event that Company agrees to the exporting, storing, or retaining of Company Data outside of such jurisdictions, Service Provider shall only do so after both parties satisfy any and all legal or regulatory requirements applicable to the location in which Company Data is exported, stored, or retained.

(b) In the event that Company Data originates in the European Economic Area or Switzerland and Company agrees that Company Data may be exported, stored, or retained outside the European Economic Area or Switzerland to a country not recognized by the European Commission as providing an adequate level of protection for Personal Data, the parties shall adhere to the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, approved by the European Commission Decision of February 5, 2010 ("SCCs"), or comply with another lawful data transfer mechanism or program. In the event the parties execute, or are subject to, the SCCs, each party acknowledges and agrees that (i) the parties obligations related to engaging with "sub-processors" (as the term is defined by the SCCs), and notification of the same, as required by the SCCs, has been satisfied pursuant to this DPA, (ii) the nature, scope, and duration of Processing as set forth in the Agreement is incorporated into Appendix 1 of the SCCs, and (iii) Appendix 2 of the SCCs shall include, at a minimum, the data security measures set forth in this DPA.

9. Privacy Policy. In the event that RPM International Inc., or any of its subsidiaries or operating companies (collectively, "RPM") collect any Personal Data from the other party that is not part of, or included in, the services or subject matter described in the Agreement, RPM shall collect and retain such Personal Data in accordance with its Privacy Policy located at [www.rpminc.com], which may be amended from time to time.

10. Indemnification. Notwithstanding any other clause in the Agreement, Service Provider shall defend, indemnify, and hold harmless Company, its affiliates, and each of their respective officers, directors, employees, agents, successors, and permitted assigns (each, a "Company Indemnitee") from, and against, all claims, losses, damages, liabilities, actions, judgments, interests, awards, penalties, costs, or expenses of whatever kind, including reasonable legal fees, against any Company Indemnitee arising out of or resulting from Service Provider's failure to comply with any of its obligations under this DPA.