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 appellation 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 a 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 but not limited to any laws governing artificial intelligence or data analytics, the California Consumer Privacy Act (the "**CCPA**") in the United States; the European Union ("EU") General Data Protection Regulation (EU) 2016/679 and its implementing laws of the EU Member States **(**collectively, the "**GDPR**"**);** and the United Kingdom (UK) 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) "**Data Subject**" means an identified or identifiable individual, directly or indirectly, whose Personal Data is being Processed by Service Provider.

(e) "**EU Standard Contractual Clauses**" means standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(f) "**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 identity, either alone or when combined with other information, an individual, a household, or a device, and that is subject to, or otherwise afforded protection under, an Applicable Data Protection Law. (g) "**Process**" means any operation 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.

(h) "**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.

(i) "**Subprocessor**" means any third-party organization engaged by Service Provider to Process Company Data on its behalf.

(j) "**UK Standard Contractual Clauses**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses VERSION B1.0, issued by the Information Commissioner under S119A(1) Data Protection Act 2018, as amended from time to time, which can be found at https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf. , and as may be amended or replaced by the UK Information Commissioner's Office or/and Secretary of State from time to time.

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 this DPA, and such Agreement(s) and this DPA represent the documented instructions of Company. Service Provider shall only Process Company Data in accordance with all Applicable Data Protection Laws, and to the minimal extent necessary 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.

(c) California Privacy. Each party acknowledges and agrees that the disclosure of Company Data to the other does not constitute, and is not the intent of either party for such disclosure to constitute, a Sale or Sharing of Company Data, and if valuable consideration, monetary or otherwise, is being provided by either party, such valuable consideration, monetary or otherwise, is being provided for the rendering of Services and not for the disclosure of Company Data. Service Provider (i) shall not collect, retain, use, or disclose Company Data for any purpose (including for any commercial purpose) other than for the specific purpose of performing the Services, unless otherwise required by law, (ii) shall not Sell or Share Company Data, except as necessary to satisfy its obligations under the Agreement, (iii) shall not collect, retain, use, or disclose Company Data outside the direct business relationship between Service Provider and Company, unless expressly permitted by law, and (iv) shall, at Company's reasonable request, cease any unauthorized Processing of Company Data and grant Company authorization to assess and remediate any such unauthorized Processing. This DPA is Service Provider's certification, to the extent the CCPA or any other Applicable Data Protection Law requires such a certification, that Service Provider understands and will comply with the Processing limitations with respect to Company Data that are reasonable and set forth in the Documented Instructions. The parties acknowledge and agree that the "business purpose" for which Service Provider Processes Company Data is to provide the Services as defined in the applicable Agreement. For purposes of this Section 3.3 only, the terms "Business," "Service Provider," "Personal Information," "Sale," and "Sell" shall have the same meaning as set forth in the CCPA (Cal. Civ. Code § 1798.140).

(d) Canadian Privacy. Service Provider shall take all reasonable steps (including implementing the procedures necessary for compliance with the Agreement and this DPA) to ensure that Service Provider (i) shall not collect, retain, use, or disclose Company Data for any purpose (including for any commercial purpose) other than for the specific purposes of carrying out the Agreement and/or performing the Services, unless otherwise required by law, and (ii) shall allow Company, on reasonable notice, to verify Service Provider's compliance relating to confidentiality requirements in the Agreement and this DPA, provided any such verification shall not be permitted to disrupt Service Provider's Processing activities or compromise the security and confidentiality of Personal Data pertaining to other Service Provider clients. The term "Security Event" shall be interpreted to include a "breach of security safeguards" and a "confidentiality incident" as each of those terms are defined and used under Applicable Data Protection Law in Canada. Notwithstanding the foregoing, Company agrees that it is aware of inconsequential attempts that might occur on a frequent basis to penetrate computer networks or servers (e.g., scans, "pings" or other inconsequential attempts) of Service Provider and Service Provider is not required to furnish Company with notice of incidents of this nature.

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 the security procedures set forth at Exhibit B.

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 Subprocessor. 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 of 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 Subprocessor. 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 engage Subprocessors to Process Company Data in accordance with this Section 7. Service Provider is hereby permitted to use the Subprocessor set forth in the Agreement or on Exhibit C hereto and will only engage other Subprocessors on the prior written authorization of Company. Service Provider shall undertake due diligence to ensure that any Subprocessor is capable of providing the level of protection for Company Data required by the Agreement and this DPA.

(b) Where Company authorizes Service Provider to engage any Subprocessors pursuant to this Section 7, the Subprocessor's activities shall be governed by a contract or other legal act that requires the Subprocessor to protect Company Data at least to the same degree that Service Provider is required to protect such Company Data. Service Provider remains liable to Company for any and all breaches or violations of this DPA caused by any such Subprocessor.

8. Data Localisation and Transfers. (a) General. Unless otherwise agreed to in writing by Company, Service Provider shall maintain, and ensure all Subprocessors 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) Data Transfers (EU Standard Contractual Clauses). To the extent Company Data originates in the European Economic Area (EEA) or in Switzerland and Service Provider a) is not established in a country which the European Commission has granted an adequacy status; and b) has not obtained Binding Corporate Rules authorization in accordance with Applicable Data Protection Law, the parties undertake to apply the provisions of the EU Standard Contractual Clauses. To the extent Company Data originates outside of the EEA and Switzerland, the parties shall also undertake to apply the provisions of the EU Standard Contractual Clauses, provided that the EU Standard Contractual Clauses are legally required and sufficient to meet the requirements of the applicable data protection regulations for the transfer of Personal Data. If the EU Standard Contractual Clauses are applicable between the parties pursuant to this Section 8(b) of this DPA, their provisions will be deemed incorporated by reference into this DPA. To the extent required by the Applicable Data Protection Laws, the parties shall enter into and execute the EU Standard Contractual Clauses as a separate document. If the parties apply and incorporate the EU Standard Contractual Clauses pursuant to this Section 8(b), then the following shall apply:

(i) The EU Standard Contractual Clauses shall be governed by the Module Two (Transfer controller to processor) clauses in all applicable instances, and the Company and/or the Company's EU affiliates shall be the data exporter and Service Provider shall be the data importer.

(ii) Each party acknowledges and agrees that Clause 7 (Optional – Docking Clause) of the EU Standard Contractual Clauses shall be deemed incorporated therein and applicable to the parties and third parties.

(iii) For purposes of Clause 9(a) (Use of sub-processors) of the EU Standard Contractual Clauses, the parties agree that Option 2 (General Authorization) shall apply to the parties, and shall be enforced in accordance with Section 7 and Exhibit C of this DPA.
(iv) For purposes of Clause 11 (Redress) of the EU Standard Contractual Clauses, the parties agree that the optional wording shall not be incorporated therein and therefore shall not be applicable to the parties.
(v) For purposes of Clause 13 of the EU Standard Contractual Clauses (Supervision), the competent supervisory authority shall be Belgium.
(vi) For purposes of Clause 17 (Governing law) of the EU Standard Contractual Clauses, the parties agree that the EU Standard Contractual Clauses shall be governed by the law of Belgium and select Clause 17, "Option 1" to this effect.
(vii) For purposes of Clause 18 (Choice of forum and jurisdiction) of the EU Standard Contractual Clauses, the parties agree that any dispute arising from the EU Standard Contractual Clauses shall be resolved by the Courts of Belgium.
(viii) Exhibits A and A-1 of this DPA shall be incorporated into Annex I of the Appendix to the EU Standard Contractual Clauses. (ix) For purposes of Annex II of the Appendix to the EU Standard Contractual Clauses, Service Provider shall implement and maintain the technical and organizational security measures set forth in this DPA, including Exhibit B. (x) The parties acknowledge that Exhibit C shall be incorporated into Annex III (List of Subprocessors) of the EU Standard Contractual Clauses and replacement Subprocessors shall be agreed upon in accordance with Section 10 of this DPA. Service Provider shall not transfer Company Data received under the EU Standard Contractual Clauses (nor permit such Company Data to be transferred) to a Subprocessor outside the EEA or Switzerland, unless the Subprocessor is established in a country which the European Commission has granted an adequacy status, provided that if the Subprocessor is not established in such a country, Service Provider shall transfer such Company Data to the Subprocessor only if: (1) it has obtained Company's prior written consent and (2) it takes such measures as necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) the Subprocessor's obtaining Binding Corporate Rules authorization in accordance with Applicable Data Protection Law, or the execution by a Subprocessor and Service Provider of the EU Standard Contractual Clauses, Module 3 (Processor to Processor).
(c) UK Standard Contractual Clauses. To the extent Company Data originates in the UK, and Service Provider is not established in the UK or a country which the UK authorities granted an adequacy status, and Service Provider has not obtained Binding Corporate Rules authorization in accordance with Applicable Data Protection Law, the parties undertake to apply the provisions of the UK Standard Contractual Clauses and hereby incorporate the UK Standard Contractual Clauses (Controller to Processor) by reference into this DPA. In case the parties can no longer rely on the UK Standard Contractual Clauses as an appropriate data transfer mechanism, the parties will conclude an alternative data transfer mechanism to replace the UK Standard Contractual Clauses, at the choice of Company, without undue delay. If the parties apply and incorporate the UK Standard Contractual Clauses pursuant to this Section 8(c), then the following shall apply:
(i) In Clause 9 of the UK Standard Contractual Clauses, the parties agree that the UK Standard Contractual Clauses shall be governed by the law of the country of the UK in which the data exporter is established, namely, England and Wales.
(ii) For purposes of the "Additional commercial clauses" of the UK Standard Contractual Clauses, the optional "Indemnification" clause is deemed incorporated therein and shall apply to the parties.
(iii) Annexes 1 and 2 of the UK Standard Contractual Clauses shall be deemed completed with the information set forth in Section 8(b) of this DPA and Exhibits A, A-1, and B of this DPA.
(iv) Each party hereby acknowledges and agrees that Section III (Local Laws and Obligations in case of access by public authorities) of the EU Standard Contractual Clauses is hereby incorporated by reference into these UK Standard Contractual Clauses.
(v) Service Provider shall not transfer any Company Data received under the UK Standard Contractual Clauses (nor permit such Company Data to be transferred) to a Subprocessor outside the UK, unless the Subprocessor is established in a country which the UK authorities have granted an adequacy status, provided that if the Subprocessor is not established in such a country, Service Provider shall transfer such Company Data to the Subprocessor only if: (1) it has obtained Company's prior written consent and (2) it takes such measures as necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) the Subprocessor's obtaining Binding Corporate Rules authorization in accordance with Applicable Data Protection Law, or the execution by a Subprocessor and Service Provider of the Standard Contractual Clauses adopted or approved by the UK Secretary of State or the UK Information Commissioner (and approved by the UK Parliament).
(d) Surveillance Disclaimers. If the parties apply and incorporate the EU Standard Contractual Clauses pursuant to Section 8(b) of this DPA or the UK Standard Contractual Clauses pursuant to Section 8(c) of this DPA, then Service Provider hereby represents and warrants the following to be true, accurate, and complete:
(i) For the purposes of 50 United States Code (U.S.C.) § 1881(4), or any other similar provision in the jurisdictions

where Service Provider is located, Service Provider is not classified as a "electronic communication service provider" or otherwise directly subject to 50 U.S.C. § 1881a ("**FISA § 702**") or to any provision with a similar effect in your country of residence.

(ii) Service Provider has never cooperated with public authorities conducting surveillance of communications pursuant to Executive Order (EO) 12333, as amended, or any other similar provision in the jurisdictions where Service Provider is located, with regard to Personal Data in Service Provider's custody or control.

(iii) Service Provider has never been the subject of a FISA § 702 warrant, or any other similar provision in the jurisdictions where Service Provider is located, with regard to a request for disclosure of any Personal Data that it Processes.

(iv) Service Provider has established internal procedures and processes for responding to FISA § 702 warrants, for cooperating with national security agencies under EO 12333, and for complying with any provision similar to either of the foregoing in the jurisdictions where Service Provider is located.

(e) Other Transfers. To the extent Company Data originates outside of the EEA, Switzerland, or the UK, and the parties seek to transfer and Process such Company Data across national borders, the parties shall also undertake to apply, as appropriate, the provisions of the EU Standard Contractual Clauses or the UK Standard Contractual Clauses to such transfer and Processing, provided that the EU Standard Contractual Clauses or the UK Standard Contractual Clauses are legally required and sufficient to meet the requirements of the Applicable Data Protection Law for the transfer and Processing of Company Data across national borders.

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 https://www.rpminc.com/privacy-policy/, which may be amended from time to time.

10. Artificial Intelligence. "AI" shall mean any technology that is designed to replicate or simulate human intelligence, including but not limited to machine learning algorithms, natural language processing, and predictive analytics. Service Provider is authorized to utilize AI in the Processing of Company Data solely for the purposes explicitly agreed upon in the Agreement or any applicable SOW/PO and with prior written consent from Client. Service Provider warrants that any use of AI in the Processing of Company Data will comply with all applicable laws including but not limited to those prohibiting discriminatory practices, privacy invasions, and intellectual property infringement. Service Provider and its affiliates and Subprocessors shall not employ any AI or algorithms that disadvantage individuals or groups based on protected characteristics such as race, gender, ethnicity, religion, age, sexual orientation, or disability. In the Processing of Company Data Service Provider shall not deploy, or permit its affiliates or Subprocessors to deploy, fully autonomous AI systems without human oversight, particularly in areas with significant potential impact on individuals. Service Provider shall implement robust security measures to safeguard all Company Data processed using AI, ensuring its confidentiality, integrity, and availability. Service Provider shall be held accountable for any errors, biases, or adverse effects arising from Service Provider's or its Subprocessors' use of AI ("AI Adverse Effects") in the Processing of Company Data. In the event of any AI Adverse Effects, Service Provider is responsible for immediate rectification and implementation of corrective measures at their own expense. Company reserves the right to conduct audits of Service Provider's AI systems and processes to verify compliance with this Agreement and/or any applicable SOW/PO. Service Provider is obligated to cooperate fully with any audits conducted by Company or its authorized representatives. Service Provider shall indemnify, defend, and hold Company harmless from any claims, liabilities, damages, or losses arising from its breach of this AI provision. Company reserves the right to terminate the Agreement or any applicable SOW/PO, in whole or in part, upon any breach of this AI provision by Service Provider, its affiliates, or its Subprocessors.

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.

Exhibit A (Data Processing Activities)

A. List of parties:

Name (Data Exporter)	Specified in the Agreement
Address	Specified in the Agreement
Contact person's name, position and contact details	Set forth in Exhibit A-1.
Activities relevant to the data transferred under these Clauses	Set forth in Exhibit A-1.
Signature and date	By executing this DPA and the Effective Date.
Role (controller / processor)	Data Controller

Name (Data Importer)	Specified in the Agreement
Address	Specified in the Agreement
Contact person's name, position and contact details	Set forth in Exhibit A-1.
Activities relevant to the data transferred under these Clauses	Set forth in Exhibit A-1.
Signature and date	By executing this DPA and the Effective Date.
Role (controller / processor)	Data Processor

B. Description of Transfer: Unless otherwise set forth in a statement of work, order form, or similar documentation, the description of the Personal Data transferred is as follows:
(i) Categories of Data Subjects: Set forth in Exhibit A-1.
(ii) Categories of Personal Data transferred: Set forth in Exhibit A-1.
(iii) Sensitive Personal Data transferred: Set forth in Exhibit A-1.
(iv) The frequency of transfer: Set forth in Exhibit A-1.
(v) Nature of Processing: software and similar IT solutions, cloud data storage, and to facilitate access and use of the Service Provider's services.
(vi) Purpose of the data transfer and further Processing: to provide access and use of the Service Provider's services.
(vii) The period for which personal data will be retained: for the duration of the Agreement and for the termination and transition period thereafter, as set forth in the Agreement.
(viii) Subprocessor transfers: the relevant information as set forth in Section 7 and Exhibit C of this DPA.

C. Competent Supervisory Authority: See Section 8(b)(v) of this DPA.

Exhibit A-1 (Data Processing Activities)

1. **Data Processing Activities** [*Briefly specify the Processing activities undertaken by Service Provider*.]

2. **Data Subjects.** The Personal Data that Service Provider Processes concerns the following categories of Data Subjects:

☐Employees (current) ☐Employees (former) ☐Customers (current)
☐Webpage users ☐Service Providers ☐Customers (potential)
☐Other:

3. **Categories of Personal Data**:

☐Name ☐Shipping Address ☐Email Address
☐Social Security No. ☐Passport number ☐Driver's License Number
☐Telephone Number ☐IP Address/Online Identifiers ☐Financial Data
☐Education Data ☐Online Behvior/Preferences ☐HR Data (employee activities)
☐Device/Usage Data ☐Date of Birth ☐Other:

4. **Special Categories/Sensitive Personal Data**:

☐Not Applicable
☐Race ☐Ethnicity ☐Political opinion ☐Religion
☐Philosophical beliefs ☐Genetic data ☐Biometric data ☐Health data
☐Sex life or orientation ☐Trade union membership

5. **The frequency of transfer:**

☐ Continuous and as often as Company uses the Service Provider's services.
☐ Other

6. **Points of Contact for Privacy Matters:**

	Name	***Title***	***Telephone***	***Email***
Company				
Service Provider				

Exhibit B (Security Controls)

Service Provider shall apply at all times the following security measures to safeguard Company Data:

1. General Obligations. Service Provider shall have reasonable security measures in place to protect the Company Data against loss and unauthorized access, misuse, interference, disclosure, alteration or other unauthorized Processing, and the Service Provider shall evaluate and improve, where necessary, the effectiveness of such safeguards. These measures include firewall, anti-virus software, malware protection and similar protections installed and kept up-to-date on all information systems used to Process the Company Data.

2. Access Control. Service Provider shall restrict access to the Company Data to employees and relevant contractors on a need-to-know basis and shall revoke access where appropriate, including from those employees whose employment is terminated.

3. Physical Security. Service Provider shall prevent unauthorized persons from gaining access to data processing systems by implementing the use of the following: a physical access control system (ID reader, magnetic card, chip card); keys; door locking (electric door openers etc.); security staff, janitors; and surveillance facilities (alarm system, video resp. CCTV monitor).

4. Technical Security. Service Provider shall prevent data processing systems from being used without authorization by implementing the use of the following: password procedures (including special characters, minimum length, frequent change of passwords); automatic blocking (e.g. password or timeout); creation of one master password per user; and differentiated access rights (profiles, roles, transactions and objects).

5. Transmission Control. Service Provider shall ensure that Company Data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check to which recipient addressee the Company Data will be transferred by using data transmission facilities. Service Provider shall implement encryption/tunneling, login/password access control, transport security, and other equivalent measures when transmitting Company Data electronically, in compliance with industry best practices and any requirements of the Applicable Data Protection Law.

6. Input control and integrity. Service Provider shall employ measures to ensure the integrity and accuracy of the Company Data, including without limitation monitoring systems able to ascertain whether Company Data has been accessed, altered or removed from data processing systems, and if so, by whom. Service Provider also shall employ measures that allow Company Data to be updated or completed pursuant to a request by the Data Subject.

7. Availability. Service Provider shall ensure that Company Data is protected against accidental destruction or loss by implementing backup procedures, uninterruptible power supply, remote storage, and disaster recovery plans.

8. Separation Control. Service Provider shall ensure that data that the exporter collected for different purposes can be Processed separately by implementing the following: “internal client” concept / limitation of use; segregation of functions production/testing; logical or physical data separation; and multitenancy.

9. Job Control and Training. Service Provider shall ensure that its employees and other personnel having access or otherwise Processing Company Data have undergone reasonably adequate training on the following: information security and the protection of Company Data; the care, handling and Processing of the Company Data; and the requirements of the Applicable Data Protection Laws.

10. Data Security Officer. Service Provider has appointed an employee or employees in charge of data security to address questions regarding data protection matters, including receiving the complaints due to any violation of, or non-compliance with, Applicable Data Protection Law.

11. Additional requirements. Service Provider agrees to abide by any additional or higher security standards that may be set forth by Applicable Data Protection Law.

Exhibit C (Subprocessors)

	Subprocessor's Name and Address	***Contact Person's Name, Title and Contact Details***	***Subject Matter and Nature of the Processing***	***Duration of the Processing***
1				
2				
3				
4				
5				