Important notice: this Schedule must be used only in Direct Materials and Technical Procurement contracts

Data Protection Schedule

This Data Protection Schedule ("**Schedule**") shall apply if it is incorporated by reference in the applicable main agreement (the "**Agreement**"). Capitalized terms that are not defined in this Schedule have the meaning ascribed to them in the Agreement.

1.1 For the purposes of this Agreement:

"**Adequacy Decision**" means a decision by the European Commission under Article 45 of the EU General Data Protection Regulation (EU 2016/679) that a country outside the EU offers an adequate level of protection.

"**Customer Personal Data**" means Personal Data that either: (i) the Customer, or a person acting on its behalf, provides to the Services, or permits the Services to access, in connection with the Agreement; or (ii) the Services creates in providing the Services.

"**Data Breach**" means any breach of security leading to the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed.

"**Data Controller**" means a person who, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means a person who Processes Personal Data on behalf of a Data Controller.

"**Data Subject**" means an identified or identifiable individual. An "identifiable" individual is one who can be identified, directly or indirectly, including by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity.

"**Personal Data**" means any information relating to a Data Subject.

to "**Process**" (and variants of it, such as "Processing") means to perform any operation or set of operations upon data, whether or not by automatic means, such as collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing (by transmission, dissemination or otherwise making available), aligning or combining, blocking, erasing or destroying.

1.2 **Appointment:** The Customer appoints the Supplier as its Data Processor. The Supplier shall Process Customer Personal Data only: (i) on behalf of the Customer; (ii) to provide the Services; (iii) so far as necessary to provide the Services; (iv) in accordance with the Customer's reasonable and documented instructions from time to time; and (v) in compliance with all applicable data protection law and for the avoidance of doubt, these terms shall not exempt the Supplier from complying with obligations to which the Supplier is subject pursuant to applicable data protection laws. The Supplier shall immediately inform the Customer in writing if it considers that any of the Customer's instructions infringe applicable data protection law.

1.3 **The Processing**: The below table describes the particulars of the Processing under the Agreement.

Particulars of the Processing	
Subject matter of the Processing:	The performance of the Agreement for Customer
Duration of the Processing:	For the term of the Agreement
Nature and purpose of the Processing:	Nature of processing: collection, recording, modification, structuring, storage, retrieval, consultation, disclosure, dissemination, combination, comparison, restriction, erasure, communication Purpose of the processing: • Information management and management of the supplier activities; • Enabling Data Subjects to use infrastructure, applications, tools and systems; • Correspondence and contact with the Data Subjects and, including administration of corresponding personal data; • Distribution or supply of products and services to third parties; and/or • Fulfilment of contractual obligations with suppliers and enforcement of their contractual obligations.
Types of Personal Data being Processed:	Business contact and system access data, i.e. personal data used for basic interactions relating to the administration and management of the Agreement, including, business contact details, name, telephone, e-mail, cell-phone number, fax, etc.), information related to billing of products and services, communications and information exchanged with such suppliers, materials and data received from such suppliers.

Categories of Data Subject to whom the Personal Data being Processed relates:	1. Suppliers, including their officers, employees and agents, advisors and other people related to them; 2. Stakeholders, including a third party with whom a business relationship is maintained, via which products or services are provided, or via which products are being sold to these third parties.

1.4 **Subprocessors**: The Supplier has the Customer's general authorization for the engagement of sub- Processor(s). The Supplier shall inform the Customer in writing of any addition or replacement of sub-Processors at least 14 days in advance, thereby giving the Customer sufficient time and relevant information to be able to object to such changes prior to the engagement of the sub-Processor(s). The Supplier shall appoint any sub-Processor in writing on terms that provide equivalent protections to those set out in this Section (including any technical and organizational measures). The Supplier shall remain fully liable to the Customer for any acts or omissions of its sub-Processors.

1.5 **Data Transfers**: The Supplier may not Process Customer Personal Data outside the Supplier's jurisdiction unless it has first: (i) obtained the Customer's prior written consent; and (ii) agreed with the Customer, and put in place, the measures which are necessary to ensure the transfer is in compliance with applicable data protection law. Where data transfers are permitted or the Supplier is incorporated outside the EEA, UK or Switzerland or country that does not have an Adequacy decision, the Supplier shall comply with the obligations set out in **Attachment 1** of this Data Protection Exhibit.

1.6 **Assistance to the Customer**: The Supplier shall, upon the Customer's request, assist the Customer to assess the impact of the Processing on the protection of Customer Personal Data, including by providing: (i) a systematic description of the way that Customer Personal Data is Processed; (ii) a description of the measures it has implemented to protect Customer Personal Data and to assist the Customer in responding to Data Subject requests; (iii) an assessment (in the form of a Data Protection Impact Assessment), of the specific risks, of which the Supplier is aware, to the rights and freedoms of Data Subjects arising out of or in connection with the Supplier's Processing; and (iv) prompt notification to the Customer if it receives any communication from any data protection authority which relates to the Processing of Customer Personal Data, or to either party's compliance with data protection law, and assist the Customer in responding to any such communication. The Supplier shall also assist the Customer as reasonably requested in cases where the Customer decides to carry out a prior consultation with the relevant data protection authority.

1.7 **Audit**: The Supplier shall make available to the Customer all information necessary to demonstrate compliance with this Section 7 and applicable data protection law and allow for and contribute to audits (including inspections) of that compliance, conducted (upon reasonable notice and within normal business hours) by the Customer or another auditor mandated by the Customer.

1.8 **Return of Customer Personal Data**: Within 14 days of the expiry (or termination) of the Agreement, the Supplier shall (at the Customer's election) destroy or return to the Customer all Customer Personal Data in its possession or control. This requirement shall not apply to the extent that the Supplier is required by any applicable law to retain some or all of the Customer Personal Data.

1.9 **Data Subjects**: The Supplier shall, if it receives any communication from any person with respect to its Processing of Customer Personal Data (including Data Subjects or data protection authorities): (i) notify the Customer within 1 business day of receiving it; (ii) provide any assistance reasonably required by the Customer to enable the Customer to respond to it; and (iii) not respond directly to it without the Customer's written permission.

1.10 **Assistance with Security Events**: The Supplier shall assist the Customer with any Data Breach and any suspected or threatened Data Breach (each, a "**Security Event**") by: (i) notifying the Customer within 24 hours of becoming aware of the Security Event at soc@pmi.com (or other address notified by the Customer in writing from time to time); (ii) providing the Customer with all relevant information and documentation in its knowledge, possession or control concerning the Security Event; and (iii) co-operating with the Customer and taking such steps as the Customer may reasonably require to assist in investigating, mitigating, and remediating any Security Event, including making any relevant notifications. The obligations set out above are without prejudice to any breach reporting obligations set out in this Agreement (including any documents incorporated by reference).

1.11 **Security**: The Supplier shall implement and maintain appropriate technical and organisational measures necessary to protect the Customer Personal Data from accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure or access, including the measures set out in the Information Security Schedule which is available at https://www.pmi.com/legal/legal-documents. The Supplier shall ensure that any person authorised to Process Customer Personal Data is bound by contractual obligations of confidentiality.

1.12 **General Restrictions:** The Supplier shall not: (i) process more than the minimum amount of Customer Personal Data necessary to perform the Services for the Customer under the Agreement; (ii) afford access to the Customer Personal Data beyond those having a "need-to-know"; (iii) duplicate or incorporate Customer Personal Data into their own records or databases except for the purpose of performing the Services for the Customer under the Agreement; (iv) have any right to process Customer Personal Data for their own commercial benefit in any form, including, without limitation, to create de-identified or anonymized data; or (v) disclose, release or transfer Customer Personal Data to any third party or business except as necessary to perform the Services for the Customer under this Agreement or as specifically directed by the Customer in writing.

Attachment 1
Standard Contractual Clauses

Exhibit Cover Sheet

1. The Parties	**Data Exporter:**	The Customer	**Data Importer:**	The Supplier
2. Master Agreement	This agreement entered into between the Data Exporter and the Data Importer ("Parties")			
3. Applicable Member State/ UK or Switzerland and Competent Supervisory Authority	Poland and Polish Law for EU England and English Law for UK FDPA and Swiss Law for Switzerland			
4. Description of Transfer	As specified in Section 1.3			
5. Categories of Data Subjects	As specified in Section 1.3			
6. Categories of Personal Data Transferred	As specified in Section 1.3			
7. Special Category Data Transferred	N/A			
8. Frequency of Transfer	As specified in Section 1.3			
9. Purpose of the Data Transfer and Further Processing	As specified in Section 1.3			
10. Period of Data Retention	Duration of the Services			
11. Transfers to Subprocessors	As specified in Section 1.4			
12. Technical Measures	As specified in Appendix 1			

Appendix 1 to Attachment 1
Technical Measures

The following contains the description of the technical and organizational measures implemented by the "data importer" (including any relevant certifications) to ensure an appropriate level of security (TOMS), taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of Data Subjects:

(a) The TOMS provided for by the following Group policies and standards (as amended from time to time):
Managing Company Information Policy
Protecting Personal Data Policy
Using Computer Hardware, Software and the Internet Policy
Managing Information Systems Policy

(b) The TOMS set out in the Group IT Policy Framework (as amended from time to time). Such Group IT Policy Framework shall in any event align to international best practice standards (NIST). Conformance to such standards shall be assessed by independent audit and risk and controls functions.

(c) Subject to stricter provisions under the foregoing paragraphs, the Data Importer shall:

- Have individuals responsible for physical and logical information security.
- Have a defined, documented, and approved logical access control policy for managing access to information systems.
- Have a documented procedure for granting/revoking/modifying access privileges for employees and contractors.
- Have a segregation of duties between individuals who request, authorize, enable and verify access.
- Enforce a password management policy for access to all platforms, applications, and databases.
- Deploy multi-factor authentication for access to platforms, applications and databases containing Personal Data.
- Deploy appropriate intrusion detection and other perimeter defence systems.
- Have a password management policy which includes password strength, password history, password resets, lockout attempts and inactivity lockouts.
- Have a privilege access provisioning and deprovisioning policy/procedure.
- Have a documented procedure for managing encryption keys and appropriate encryption protection.
- Encrypt removable media storage devices (e.g., pen drive, CD/DVD, USB portable devices, and back up tapes) used for storing Data Importer data.
- Have contract(s) with subcontractors or any other subprocessors of data which covers the standard requirements (e.g., data protection, NDA, confidentiality agreement, information security, business continuity etc.).
- Use Mobile Devices Management on corporate mobile devices.
- Have a documented third-party information security risk management procedure to manage risk associated with subcontractors.
- Have a process to review subcontractor's performance and monitor security requirements defined as per contract and/or service level agreement.
- Have access for all staff (employees, contractors and visitors) controlled through the use of physical controls such as security officers, alarms and badge access.
- Have individuals assigned with responsibility for storing and monitoring access control logs using physical security monitoring devices.
- Have a documented process for performing data backups and creating, updating and reviewing disaster recovery plans for critical systems.
- Have capability to maintain an audit trail of important key events including:
  - Logon/logoff events
  - Changes to access rights (role definitions, allocation of roles)
  - Changes to audit log (configuration, deletion, etc.)
  - Any other key transactions.
- Regularly review and audit IT platforms, applications and databases containing Personal Data including the conducting of vulnerability assessments.
- Have a hardening process and procedure to manage configuration of infrastructure, network, applications, and end user devices.
- Have a tested and appropriate incident response process to identify and respond to incidents involving Personal Data with appropriate legal oversight.
- Provide training to employees on data privacy and information classification.
- Provide security awareness training to employees.
- Data protection aspects are established as an integral part of corporate risk management.
- A data protection policy and related guidance notes are maintained centrally and available to all employees.

1. **Definitions.** Unless otherwise defined in these Standard Contractual Clauses, capitalized terms have the same meaning as in the GDPR.

1.1. "Applicable Law" shall mean the law of the applicable Member State, Switzerland or UK as specified in the Exhibit Cover Sheet.

1.2. "Clauses" shall mean the SCC clauses.

1.3. The "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC or the UK or Swiss equivalent legislation as applicable.

1.4. The "SCC" or "SCCs" means the Standard Contractual Clauses set out in the annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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.

2. **SCCs incorporated by reference**. The Parties hereby agree to incorporate the SCCs (including where relevant the UK Appendix) by reference.

3. **Applicable Modules in the SCCs.** Based upon the relationship and status of the Data Exporter and Data Importer with regards to the Personal Data that may be transferred under this Exhibit and the SCCs, the SCCs must be read with the following module(s) in effect, and that all other modules below and in the SCCs shall be inoperative:

3.1. **Data Exporter as Controller and Data Importer as Controller**. Module 1 shall apply, and Modules 2 through 4 of the SCCs are inoperative.

3.1.1. For purposes of Clause 13(a) where:

3.1.1.1. the Data Exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority; or

3.1.1.2. the Data Exporter is established in Switzerland: The FDPIC shall act as the competent supervisory authority with responsibility for ensuring compliance by the data exporter with Swiss law as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

3.1.2. For purposes of Clauses 14 through 16, the bracketed language shall not apply unless expressly pertaining to Module 1.

3.1.3. For purposes of Clauses 17 and 18, the Parties agree to OPTION 1 (for Clause 17) and, where required to specify the Member State in Clauses 17 and 18(b), select the law and courts as specified in Section 3 of the Cover Page to this Exhibit. The term 'member state' in Clause 18(c) must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland).

3.2. **Data Exporter as Controller and Data Importer as Processor.** Module 2 shall apply, and Modules 1, 3, and 4 of the SCCs are inoperative. In addition:

3.2.1. For purposes of Clause 9(a), the Parties select "OPTION 2: GENERAL WRITTEN AUTHORISATION," and Data Importer shall inform the Data Exporter in writing at least 7 days in advance of any intended changes to the agreed list referenced in OPTION 2 to Clause 9(a) and as specified in Section 11 of the Cover Page of this Exhibit. Data Exporter's authorization shall be deemed given unless the Data Exporter objects to Data Importer within the allotted time period.

3.2.2. For purposes of Clause 13(a), where

3.2.2.1. the Data Exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority; or

3.2.2.2. the Data Exporter is established in Switzerland: The FDPIC shall act as the competent supervisory authority with responsibility for ensuring compliance by the data exporter with Swiss law as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

3.2.3. For purposes of Clauses 14 through 16, the bracketed language shall not apply unless expressly pertaining to Module 2.

3.2.4. For purposes of Clauses 17 and 18, the Parties agree to OPTION 1 (for Clause 17) and, where required to specify the Member State in Clauses 17 and 18(b), select the law and courts as specified in Section 3 of the Cover Page to this Exhibit. The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland or the UK from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c.

3.3. **Data Exporter as Processor and Data Importer as Processor.** Module 3 shall apply, and Modules 1, 2, and 4 of the SCCs are inoperative. In addition:

3.3.1. For purposes of Clause 9(a), the Parties select "OPTION 2: GENERAL WRITTEN AUTHORISATION," and Data Importer shall inform the Controller in writing seven (7) days in advance of any intended changes to the agreed list referenced in OPTION 2 to Clause 9(a) and as specified in Section 11 of the Cover Page of this Exhibit. The Data Exporter's authorization shall be deemed given unless the Data Exporter objects to Supplier within the allotted time period.

3.3.2. For purposes of Clause 13(a), where:

3.3.2.1. the Data Exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority; or

3.3.2.2. the Data Exporter is established in Switzerland: The FDPIC shall act as the competent supervisory authority with responsibility for ensuring compliance by the data exporter with Swiss law as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

3.3.3. For purposes of Clauses 14 through 16, the bracketed language shall not apply unless expressly pertaining to Module 3 of the SCCs.

3.3.4. For purposes of Clauses 17 and 18, the Parties agree to OPTION 1 (for Clause 17) and, where required to specify the Member State in Clauses 17 and 18(b), select the law and courts as specified in Section 3 of the Cover Page to this Exhibit. The term 'member state' in Clause 18(c) must not be interpreted in such a way as to exclude data subjects in Switzerland or the UK from the possibility of suing for their rights in their place of habitual residence (Switzerland or the UK).

3.4. **Data Exporter as Processor and Supplier/Data Importer as Controller.** Module 4 shall apply, and Modules 1 through 3 are inoperative. In addition:

3.4.1. Clauses 14 and 15 will apply only to the extent the Data Exporter is collecting Personal Data in the European Economic Area, UK or Switzerland.

3.4.2. For purposes of Clauses 14 through 16, if applicable, the bracketed language shall not apply unless expressly pertaining to Module 4.

3.4.3. For purposes of Clauses 17 and 18, where required to specify the country, the Parties select the law and courts as specified on the Exhibit Cover Sheet.

4. **Inclusion of Docking Clause.** The Parties agree to include Clause 7.

5. **Annexes.** For purpose of Annex I, Annex II, and Annex III of the SCCs:

5.1. **Annex I: List of Parties, Description of Transfer, and Competent Supervisory Authority.** All as specified in the Exhibit Cover Sheet.

5.2. **Annex II: Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data:** All as specified in the Exhibit Cover Sheet.

5.3. **Annex III: List of Sub-Processors.** As specified in the Exhibit Cover Sheet

UK APPENDIX

BACKGROUND

This International Data Transfer Addendum to the EU Commission Standard Contractual Clauses is adapted from a document published by the UK ICO at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ VERSION B1.0, in force 21 March 2022.

PART 1: TABLES

Table 1: Parties

1. The Start date is the start date of the Master Agreement
2. The Parties
   - 2.1. Exporter and Exporter Key Contact means the party identified as 'Data Exporter' in the Exhibit Cover Sheet.
   - 2.2. Importer and Importer Key Contact means the party identified as 'Data Importer' in the Exhibit Cover Sheet.

Table 2: Selected SCCs, Modules and Selected Clauses

1. Addendum EU SCCs means the SCCs identified in the Exhibit Terms.

Table 3: Appendix Information

1. "Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:
   - 1.1. Annex 1A: List of Parties: per Exhibit Cover Sheet.
   - 1.2. Annex 1B: Description of Transfer: per Exhibit Cover Sheet.
   - 1.3. Annex II: per Technical and organisational measures including technical and organisational measures to ensure the security of the data: per Attachment to the Exhibit Cover Sheet**, Technical Measures**
   - 1.4. Annex III: List of Sub-processors (Modules 2 and 3 only): per Exhibit **Cover Sheet.**

Table 4: Ending this Addendum when the Approved Addendum Changes

1. Which Parties may end this Addendum as set out in Section 19: neither Party.

PART 2: MANDATORY CLAUSES

1. Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.