# Supplier Data Processing Agreement

This Data Processing Agreement ("**DPA**") is made by and between the Supplier identified in the relevant Master Services and/or Product Agreement(s) and its affiliates, subsidiaries, and/or operating companies (collectively "**Supplier**"), and **Vontier Business Services LLC** and its affiliates, subsidiaries, and/or operating companies (collectively "**Vontier**"), having a place of business at 5438 Wade Park Blvd., Suite 600, Raleigh, North Carolina 27607 USA and is effective from the effective date of the relevant Master Services and/or Product Agreement(s) between the Supplier and Vontier ("**Agreement**").

As Supplier and Vontier have entered into the Agreement, which may require the Processing of Personal Information by Supplier acting as Service Provider (as defined under applicable Data Protection Laws) ("**Processor**") for or on behalf of Vontier acting as the Business (as defined under applicable Data Protection Laws) and/or its customers (if applicable) ("**Controller**"), this DPA will set out the additional requirements, terms, and conditions on which the Processor will process Personal Information until such time the Processor ceases all Processing of Personal Information on behalf of the Controller.

## 1. Definitions and interpretation

Capitalized terms used but not defined in this DPA shall have the meaning set forth in the Agreement. Where different definitions for the same term have been used in the Agreement and this DPA, the definitions provided in this DPA shall prevail in relation to the terms of this DPA. In this DPA, the following words and phrases shall have the following meaning unless the context otherwise requires:

"**Controller Personal Information**" means all Personal Information and Personal Data, in whatever form or medium, which is Processed by the Processor for and on behalf of the Controller and/or the Controller's customers (if applicable) whether or not such Personal Information and Personal Data is supplied to (by transfer or access), and/or produced or generated by or on behalf of the Processor in connection with the Agreement or this DPA, including as set out in Appendix 1.

"**Data Subject**", "**Personal Data**", "**Business**", "**Service Provider**", "**Personal Information**", "**Personal Data Breach**", "**Processing**" and "**Sensitive Personal Information**" (or "**Special Categories of Personal Data**") all have the meanings given to those terms in applicable Data Protection Laws (and related terms, such as "Process", have corresponding meanings). If any of these terms are not defined under applicable Data Protection Laws, the term shall have the meaning given to it under the GDPR. Where this DPA uses the term "Controller," it shall be read to include "Data Fiduciary" as defined under the DPDPA in the context of Indian data processing. Where this DPA uses the term "Data Subject," it shall be read to include "Data Principal" as defined under the DPDA. Where this DPA uses the term "Processor," it shall be read to include "Data Processor" as defined under the DPDPA. These equivalences are established for interpretive clarity and do not alter the substantive obligations of either party.

"**Data Exporter**" has the meaning set out in the EU Standard Contractual Clauses.

"**Data Importer**" has the meaning set out in the EU Standard Contractual Clauses.

"**Data Protection Laws**" means all laws, regulations, legislative and regulatory requirements, and legally binding codes of practice applicable to the Processing, privacy, integrity, security, confidentiality and use of the Controller Personal Information, as applicable to Controller, the Controller's customers and/or the Supplier including, without limitation and where applicable (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR") together with national implementing laws in any Member State of the European Economic Area ("EEA"); (ii) the GDPR as it is incorporated into the laws of the United Kingdom; (iii) the UK Data Protection Act of 2018; (iv) the Swiss Federal Act on Data Protection; (v) United States laws and regulations, including but not limited to the California Consumer Privacy Act, as amended by the California Privacy Rights Act and Section 5(a) of the Federal Trade Commission Act (15 U.S.C. § 45); (vi) the Lei Geral de Proteção de Dados of Brazil (13709/2018); (vii) the Protection of Personal Information Act 2013 of South Africa; (viii) India's Digital Personal Data Protection Act of 2023 ("DPDPA"); and any legislation, regulation, or authoritative guidance that supplements, amends, or supersedes the foregoing.

"**EU Standard Contractual Clauses**" means the clauses, approved with Commission Implementing Decision (EU) 2021/914 of June 4, 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, as amended, updated, or replaced by the European Commission, as incorporated in Appendix 3 (a copy of which is available at: www.vontier.com/EU_Contractual_Clauses).

"**Services**" shall have the meaning given to it under the Agreement or where this term is not defined means the services described in the Agreement and agreed between the Controller and the Processor from time to time.

"**Supervisory Authority**" means any competent data protection or privacy authority in any jurisdiction in which the Controller, the Controller's customers (if applicable) or the Processor is established, the Processor provides the Services, or in which the Processor Processes Controller Personal Information.

"**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under s. 119A(1) of the UK Data Protection Act 2018, as may be amended or superseded from time to time, as incorporated in Schedule 5 of Appendix 3 (a copy of which is available at: www.vontier.com/EU_Contractual_Clauses).

**2. Appointment and role of the parties**

2.1 The Controller appoints the Processor to Process Controller Personal Information on its behalf as is necessary for the provision of the Services and performance of the Agreement. Other than as set out herein, the Processor shall not Process the Controller Personal Information for any other incompatible purpose.

**3. Details of the Processing**

3.1 Processing of the Controller Personal Information by the Processor under this DPA shall be for the: (a) subject-matter; (b) duration; (c) nature and purpose; and (d) the type of Personal Information and categories of Data Subjects, as set out in this DPA.

3.2 The nature, purpose, and instructions of processing are described in Appendix 1.

3.3 The obligations and rights of the Controller are set out in this DPA and in Data Protection Laws.

**4. Complying with Data Protection Laws**

4.1 Each party shall in all cases Process Controller Personal Information in compliance with Data Protection Laws.

4.2 The Controller shall have the right to take reasonable and appropriate steps to help ensure that the Processor uses the Controller Personal Information in a manner consistent with the Controller's obligations under Data Protection Laws.

4.3 The Controller shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Controller Personal Information.

4.4 The Processor hereby agrees to notify the Controller immediately, but in any event no later than forty-eight (48) hours from the time it makes a determination, if it determines that it can no longer meet its obligations under Data Protection Laws.

4.5 Neither party shall cause the other party, by act or omission, to breach any Data Protection Laws.

4.6 If any of the Data Protection Laws in any country to which this DPA relates conflict, the requirements of the country that necessitates stricter or additional requirements to protect Controller Personal Information shall be applied.

**5. Acting on controller's documented instructions**

5.1 The Processor shall Process Controller Personal Information only on the documented instructions of the Controller including as set out in this DPA and the Agreement. The Processor also has the right to Process the Controller Personal Information to the extent required by law,

following Processor's prior notification to the Controller, except where mandatory law prohibits such notification. The Processor shall promptly notify the Controller if in the Processor's reasonable opinion any instruction from the Controller infringes Data Protection Laws, with such notification to include an explanation of why Processor has formed such an opinion.

5.2 The Processor acknowledges that it is prohibited from:

(A) selling or sharing Controller Personal Information unless otherwise permitted under Data Protection Laws or this DPA;

(B) retaining, using, or disclosing Controller Personal Information for any purpose other than for the purpose(s) specified in Appendix 1 or as otherwise permitted under Data Protection Laws; or,

(C) combining Controller Personal Information with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the Data Subject, unless otherwise allowed under Data Protection Laws or this DPA.

**6. Ensuring employee confidentiality**

The Processor shall ensure that any person acting under its authority who may have access to, or who otherwise Process, Controller Personal Information are subject to legally binding obligations of confidentiality, and at all times act in compliance with Data Protection Laws and shall ensure that such persons receive regular and appropriate training on the same.

**7. Taking appropriate technical and organizational measures**

7.1 The Processor shall implement appropriate technical and organizational measures:

(A) designed to assist the Controller in responding to requests from Data Subjects to exercise their rights under Data Protection Laws; and

(B) designed to ensure a level of security for the Controller Personal Information appropriate to the risk posed by the Processor's Processing of such Controller Personal Information, to protect it from unauthorized, accidental or unlawful disclosure, access, loss, or alteration, and shall include the measures set out in Appendix 2 at a minimum.

**8. Data breach notification and assistance**

8.1 The Processor shall notify Controller in writing without undue delay if it becomes aware of a Personal Data Breach affecting the Controller Personal Information (a "**Data Breach**"), and provide the Controller, as soon as reasonably practicable with the following information relating to the Data Breach:

(A) the nature of the Personal Information affected;

(B) the categories and number of Data Subjects concerned;

(C) the number of Personal Information records concerned;

(D) measures taken to address the Data Breach; and

(E) the possible consequences and adverse effect of the Data Breach.

(F) The Processor, at its own cost, shall provide Controller with all reasonable assistance in relation to Controller's compliance with Articles 32-34 of the GDPR or equivalent requirements of other Data Protection Laws. The Processor shall provide such assistance in a timely manner and in accordance with any time frames set out in Data Protection Laws.

**9. Subcontracting**

9.1 The Controller hereby authorizes the Processor to engage third parties to perform Processing activities in respect of Controller Personal Information on behalf of the Controller ("Subprocessors"). The Processor shall notify the Controller in writing in advance if it intends to

replace or add to the Subprocessors and the Controller shall have a right, acting reasonably, to reject to such replacement or additional Subprocessor. If the Controller does not notify the Processor in writing of its objection to the additional or replacement Subprocessor within twenty (20) days of being notified of such addition or replacement, the Processor may proceed with engaging the additional or replacement Subprocessor to Process the Controller Personal Information. If the Controller notifies the Processor of its objection in accordance with this Clause, the parties shall work in good faith to find a resolution to the issue. If a resolution cannot be reached within thirty (30) days of the Controller's objection, either party has the right to terminate this DPA and the Agreement on thirty (30) days' written notice to the other.The Processor shall enter into a written agreement with each Subprocessor that contains obligations that are consistent with and, at a minimum, no less than the responsibilities and requirements set out in this DPA.

9.2 The Processor shall promptly provide, on request, the relevant details of any such written agreements between the Processor and its Subprocessors.

9.3 The Processor shall remain fully liable to Controller for any non-compliance with the terms of this DPA by any Subprocessor.

**10. Cross Border Transfers of Personal Information**

10.1 The Processor shall not, and shall procure that any Subprocessor shall not, transfer any Controller Personal Information to any country or territory outside the Controller Personal Information's country or territory of origin, without first ensuring that appropriate safeguards are in place to protect the Controller Personal Information, in accordance with the requirements of this DPA and applicable Data Protection Laws.

10.2 Subject to 10.4 and 10.5 (as applicable), if Controller Personal Information originating from the EEA, UK or Switzerland is transferred from the Controller to the Processor as part of this DPA and/or the Agreement, Module Two of the EU Standard Contractual Clauses is hereby incorporated into this DPA by reference and shall apply to the Controller as the Data Exporter and to the Processor as the Data Importer.

10.3 Subject to 10.4 and 10.5 (as applicable), if Controller Personal Information originating from the EEA, UK or Switzerland is transferred from the Processor to the Controller as part of this DPA and/or the Agreement, Module Four of the EU Standard Contractual Clauses is hereby incorporated into this DPA by reference and shall apply to the Processor as the Data Exporter and to the Controller as the Data Importer.

10.4 With respect to Controller Personal Information originating from Switzerland, the EU Standard Contractual shall be amended as follows: (i) the term "Member State" will 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) in accordance with Clause 18(c) of the EU Standard Contractual Clauses; and (ii) references to "Regulation (EU) 2016/679" or "that Regulation" will be understood as references to the Swiss Federal Act on Data Protection; (iii) all references to the "Commission" shall be deemed to refer to the Federal Data Protection and Information Commissioner; (iv) all references to the "European Union", "EU", "Member State" and "Union" shall be deemed to refer to Switzerland; and (v) the footnotes are removed.

10.5 With respect to Controller Personal Information originating from the UK, the EU Standard Contractual Clauses shall be amended in accordance with the UK Addendum.

10.6 With respect to Controller Personal Information originating from India, the parties shall not transfer Personal Data of Indian data principals to any country outside India except to countries permitted under Section 16 of the DPDPA, as notified by the Central Government from time to time. Pending formal notification of permitted countries, the parties shall ensure that any cross-border transfer of Indian Personal Data is subject to contractual obligations on the recipient that

are functionally equivalent to those under this DPA and the DPDPA.

10.7 With respect to Controller Personal Information originating from the United States, Processor shall ensure not to transfer, sell, or grant access to any such Controller Personal Information to any individual or organization located in China, Russia, Iran, North Korea, Cuba, Venezuela, or any other sanctioned person, entity, or territory, as prescribed by the Bulk Data Rule, 28 CFR Part 202 ("Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons").

**11. Deleting or returning of Controller Personal Information**

11.1 The Processor shall promptly and in any event within thirty (30) days: (a) of termination or expiry of the Agreement, for whatever reason; (b) after the end of the provision of the relevant Services related to the Processing; or (c) if earlier, as soon as Processing by the Processor of any Controller Personal Information is no longer required for the Processor's performance of its obligations under this Agreement, cease all use of such Controller Personal Information and shall either securely destroy or return to the Controller (at the Controller's direction) all such Controller Personal Information.

**12. Records and audit**

12.1 The Processor shall maintain complete, accurate and up to date written records of all Processing activities carried out on behalf of the Controller and shall make available to the Controller, on written request, such records and any other information as is reasonably required by Controller to demonstrate compliance by the Processor with its obligations under this DPA and applicable Data Protection Laws.

12.2 The Controller has the right to conduct, by itself or by an independent third party acting under Controller's direction that is not a competitor of the Processor, at Controller's cost, an inspection, including an audit, of the Processor's data security and privacy procedures relating to the Processing of Controller Personal Information and compliance with this DPA. Such inspection or audit may only occur once per calendar year, during the Processor's normal business hours following receipt by the Processor of thirty (30) days prior written notice of such inspection and audit. For the avoidance of doubt, such inspection or audit shall not cause unreasonable disruption to the Processor's business and shall not include an inspection or audit which compromises Personal Information or confidential information Processed by the Processor on behalf of third parties.

**13. Informing Controller of complaints, enquiries and third-party access requests**

13.1 To the extent not prohibited by applicable law, the Processor shall inform the Controller without undue delay of any enquiry, complaint, notice or other communication it receives from any Supervisory Authority or any Data Subject in connection with the Processor's Processing of the Controller Personal Information. The Processor shall provide all reasonable assistance to Controller to enable Controller to respond to such enquiries, complaints, notices or other communications and to comply with Data Protection Laws. For the avoidance of doubt, the Processor shall not respond to any such enquiry, complaint, notice or other communication without the prior written consent of Controller unless required to do so under applicable law.

13.2 Subject to 13.6, the Processor shall notify the Controller without undue delay if it:

(1) receives a request from a public authority, including judicial authorities, for the disclosure of Controller Personal Information ("**Public Authority Request**"); such notification shall include, but is not limited to, information about the Controller Personal Information requested, the requesting authority, the legal basis for the request and the Processor's proposed response; or

(2) becomes aware of any direct access by public authorities to Controller Personal Information; such notification shall include all information available to the Processor

about such access, including but not limited to, the timing and method of the access, the Controller Personal Information accessed, the reason for the access and all communications with the public authority about such access (if any).

13.3 The Processor shall review the legality of the Public Authority Request, whether it is within the powers granted to the requesting public authority, and if, after careful assessment by or on behalf of the Processor:

(1) the Processor concludes that there are reasonable grounds to consider that the Public Authority Request is unlawful, the Processor must challenge the request; or

(2) the Processor concludes that the Public Authority Request is lawful, the Processor must pursue possible grounds of appeal.

When challenging a Public Authority Request, the Processor shall use best efforts to seek interim measures with a view to suspending the effects of the Public Authority Request until the competent judicial authority has decided on the merits of the Public Authority Request. The Processor shall not disclose the Controller Personal Information requested until required to do so under the applicable legal procedural rules.

13.4 The Processor shall document the assessment set out in 13.3 and any challenge to or appeal against the Public Authority Request and, to the extent not prohibited by law, make such documentation available to the Controller on request.

13.5 The Processor shall provide the minimum amount of Controller Personal Information permissible when responding to a Public Authority Request, based on a reasonable interpretation of the request.

13.6 If the Processor is legally prohibited from notifying the Controller in accordance with 13.2, the Processor shall use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible about the notifiable matter, as soon as possible, to the Controller. The Processor shall document its best efforts in order to be able to demonstrate them on request from the Controller.

**14. General Terms**

14.1 This DPA constitutes the entire agreement between the parties and supersedes, terminates and extinguishes all previous and contemporaneous agreements, promises, assurances and understandings between them, whether written or oral, relating to its subject matter.

14.2 Both Parties acknowledge and understand that the Controller Personal Information may be subject to Data Protection Laws that require certain undertakings and/or the entering into of agreements, including in relation to the cross-border transfer of the Controller Personal Information. Both parties agree that they shall enter into any alternative or additional agreements or arrangements or implement any additional measures as may be required under Data Protection Laws in relation to the Processing and/or cross-border transfer of the Controller Personal Information.

14.3 In the event of any conflict between the provisions of this DPA, the Agreement and the EU Standard Contractual Clauses the following order of precedence shall apply: the EU Standard Contractual Clauses; the provisions of this DPA and then the Agreement.

14.4 Variation or amendment of this Agreement is only valid upon the signed written agreement of both parties.

14.5 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or

unenforceable part had never been contained therein.

14.6 The Processor agrees to indemnify, keep indemnified and defend at its own expense the Controller against all costs, claims, damages or expenses directly incurred by the Controller as a result of failure by the Processor to comply with any of its obligations under this DPA and/or Data Protection Laws.

14.7 Except where the parties cannot limit or exclude their liability under applicable law, each party's liability in the aggregate arising out of or in connection with this DPA, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is subject to the limitations and exclusions of liability in the Agreement, and any reference in the Agreement to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and the DPA together.

14.8 Any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with this DPA shall be governed by the laws set out in the Agreement and the courts in the territory set out in the Agreement shall have jurisdiction to resolve such disputes or claims.

## Appendix 1:
## Details of Processing of Controller Personal Information

This Appendix 1 includes certain details of the Processing of Controller Personal Information as required by Article 28(3) GDPR or equivalent requirements of other Data Protection Laws.

**1. Subject matter and duration of the Processing of Controller Personal Information**

The subject matter of the Processing of the Controller Personal Information is the provision of the Services to the Controller. Controller Personal Information will be Processed for the duration of the Agreement between the parties, subject to this DPA.

**2. Nature and purpose of the Processing of Controller Personal Information**

Processor shall host, maintain and otherwise process Controller Personal Information only in connection with the provision of Services pursuant to the terms of the Agreement and this DPA.

**3. Types of Controller Personal Information Processed**

Personal Information input by (or at the direction of) the Controller or by Data Subjects into Processor's system or that Processor otherwise Processes on Controller's behalf in connection with providing the Services pursuant to the terms of the Agreement and this DPA, including first and last name, business contact information (including, but not limited to: company, email phone, physical business address) and other Controller Personal Information as may be required to provide the Services, or as otherwise instructed by Controller.

**4. Categories of Data Subject to whom the Controller Personal Information Relates**

Controller's employees, contractors, customers, and Controller's customer's end users.

**5. Countries in which the Processor will Process the Controller Personal Information**

Supplier's location and those countries in accordance with Supplier's obligations under this DPA.

VONTIER™

## Appendix 2:
## Technical and Organizational Measures to Ensure the Security of the Data

| Technical Measures to Ensure Security of Processing | |
|---|---|
| **1. Inventory and Control of Hardware Assets** | Actively manage all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. |
| **2. Inventory and Control of Software Assets** | Actively manage all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution. |
| **3. Continuous Vulnerability Management** | Continuously acquire, assess, and take action on new information in order to minimize the window of opportunity for attackers. |
| **4. Controlled Use of Administrative Privileges** | Maintain processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, applications, and data. |
| **5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** | Implement and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |
| **6. Maintenance, Monitoring, and Analysis of Audit Logs** | Collect, manage, and analyze audit and security logs of events that could help detect, understand, or recover from a possible attack. |
| **7. Email and Web Browser Protections** | Deploy automated controls to minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems or content. |
| **8. Malware Defenses** | Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. |
| **9. Limitation and Control of Network Ports, Protocols, and Services** | Manage (track, control, correct) the ongoing operational use of ports, protocols, services, and applications on networked devices in order to minimize windows of vulnerability and exposure available to attackers. |
| **10. Data Recovery Capabilities** | Maintain processes and tools to properly back up personal data with a proven methodology to ensure the confidentiality, integrity, availability, and recoverability of that data. |
| **11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches** | Implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |
| **12. Boundary Defenses** | Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data. |
| **13. Data Protection** | Maintain processes and tools used to prevent data exfiltration, mitigate the effects of exfiltration, and ensure the confidentiality and integrity of data. |
| **14. Controlled Access Based on the Need to Know** | Maintain processes and tools to track, control, prevent, and correct secure access to critical or controlled assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these assets based on an approved classification. |
| **15. Wireless Access Control** | Maintain processes and tools to track, control, prevent, and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems. |
| **16. Account Monitoring and Control** | Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimize opportunities for unauthorized, inappropriate, or nefarious use. |

| Organizational Measures to Ensure Security of Processing | |
|---|---|
| **1. Implement a Comprehensive Information Security Program** | Through the implementation of a Comprehensive Information Security Program (CISP), maintain various administrative safeguards to protect personal data. These measures are designed to ensure:<br>• security, confidentiality and integrity of personal data<br>• protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud<br>• that employees, contractors, consultants, temporaries, and other workers who have access to personal data only process such data on instructions from the data controller. |
| **2. Implement a Security Awareness and Training Program** | For all functional roles (prioritizing those mission critical to the business, its security, and the protection of personal data), identify the specific knowledge, skills and abilities needed to support the protection and defense of personal data; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs. |
| **3. Application Software Security** | Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. |
| **4. Incident Response and Management** | Protect the organization's information, including personal data, as well as its reputation, by developing and implementing an incident response infrastructure (*e.g.*, plans, defined roles, training, communications, management oversight, retainers, and insurance) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the organization's network and systems. |
| **5. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises** | Test the overall strength of the organization's defense (the technology, processes, and people) by simulating the objectives and actions of an attacker; as well as, assess and validate the controls, policies, and procedures of the organization's privacy and personal data protections. |
| **6. Physical Security and Entry Control** | Require that all facilities meet the highest level of data protection standards possible, and reasonable, under the circumstances relevant to the facility and the data it contains, process, or transmits. |

## Appendix 3:
## EU Standard Contractual Clauses

The EU Standard Contractual Clauses and related Annexes as well as the UK Addendum are available at: www.vontier.com/EU_Contractual_Clauses and are incorporated and integrated into this Agreement.