Distributor Data Privacy Agreement

This Distributor Data Privacy Agreement ("**Agreement**") is made by and between:

A. **Distributor**, as identified in the relevant Distributor and/or Reseller Agreement or similar, and its affiliates, subsidiaries, and/or operating companies (collectively "**Company A**"); and,

B. **Vontier Business Services LLC** and its affiliates, subsidiaries, and/or operating companies having a place of business at 5438 Wade Park Blvd., Suite 600, Raleigh, North Carolina 27607 USA (collectively "**Company B**"), (each a "**Party**", together, "**the Parties**"), as of the date of the last signature thereof below.

WHEREAS, the Parties have executed the Contract which may require the Processing of Personal Information, the Parties now agree to the following terms and conditions with respect to the Processing of Personal Information:

1. **Definitions and Interpretation**

For the purpose of this Agreement, the following words and phrases shall have the following meaning unless the context otherwise requires:
"**Contract**" means the Distributor and/or Reseller Agreement or similar between Company A and Company B.
"**Data**" means the Controller Personal Information as described in Schedule 1.
"**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 the Parties 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 ("CCPA"), as amended by the California Privacy Rights Act ("CPRA") 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 Schedule 3 (a copy of which is available at: www.vontier.com/EU_Contractual_Clauses).
"**Permitted Purpose**" means the purpose(s) for which the Controller Personal Information may be Processed as set out in Schedule 1.
"**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 3 (a copy of which is available at: www.vontier.com/EU_Contractual_Clauses).
"**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.

2. **Scope of Processing**

2.1. The aim of sharing the Controller Personal Information is to facilitate the provision and receiving of services under the Contract, to enrich the Data Recipient's understanding of its customers, which will allow it to offer more suitable products and services, and to help enhance and improve the Data Recipient's goods and/or services (the "**Aim**").

2.2. The Parties acknowledge that in connection with the Aim, the Data Receiver may receive from the Data Discloser Personal Data and/or Personal Information about or related to certain Data Subjects as more particularly described in Schedule 1 (collectively "**Controller Personal Information**").

2.3. The Data Discloser warrants that the Controller Personal Information it provides to the Data Receiver will, to the best of its knowledge, be accurate and agrees to notify the Data Receiver promptly, after being made aware, of any inaccuracies in the Controller Personal Information.

2.4. The Data Discloser undertakes not to provide the Data Receiver with any Personal Data and/or Personal Information that is not described in Schedule 1.

2.5. The Data Receiver:

2.5.1. may only process the Controller Personal Information for the Permitted Purpose; and,

2.5.2. shall not Process the Controller Personal Information for any purpose that is incompatible with the Permitted Purpose.

3. Relationship of the Parties

3.1. The Parties acknowledge that each Party shall process the Controller Personal Information as a separate and independent Controller (or Business, where applicable), for its own purposes and in its own right and in the case of the Data Receiver, only for the Permitted Purpose. In no event will the Parties process the Controller Personal Information as joint Controllers (as that term is understood under the GDPR).

3.2. the Party or Parties sharing the Controller Personal Information are "**Data Disclosers**" and each a "**Data Discloser**"; and,

3.3. the Party or Parties receiving the Controller Personal Information are "**Data Receivers**" and each a "**Data Receiver**".

3.4. Nothing in this Agreement shall limit the Data Discloser from collecting or using the Controller Personal Information, or other Personal Data and Personal Information, that Data Discloser otherwise Processes independently of Data Receiver and the Aim.

4. Responsibilities

4.1. **Transparency.** Data Discloser shall, prior to sharing any Controller Personal Information with the Data Receiver:

4.1.1. provide all necessary disclosures, information or notices to the Data Subjects to satisfy the requirements of Data Protection Laws. Without prejudice to the generality of the foregoing, such disclosure, information or notice shall, at a minimum, include the following information: (i) the type of Controller Personal Information collected, shared, sold or otherwise Processed by Data Discloser and the Permitted Purpose of Processing thereof; (ii) the categories of recipients who will have access to or receive the Controller Personal Information; including the Data Receiver; (iii) where applicable, the legitimate interests pursued by the Data Discloser in Processing the Controller Personal Information, including sharing the Controller Personal Information with the Data Receiver; and (iv) any other information the Data Discloser is required to provide to the Data Subjects under Data Protection Laws to allow it to lawfully disclose the Controller Personal Information to the Data Receiver; and,

4.1.2. make available to the Data Receiver, all such disclosures, information and notices provided to Data Subjects. The Data Receiver may terminate this Agreement without prejudice to any rights or remedies if, in the Data Receiver's sole discretion, the Data Receiver concludes

that such disclosures, information and notices do not meet applicable Data Protection Laws.

4.2. **Lawfulness.** If the Data Discloser is relying on the Data Subject's consent to share the Controller Personal Information with the Data Receiver:

4.2.1. the Data Discloser will make available to the Data Receiver, for the Data Receiver's review prior to its use, all such permissions and consents. The Data Receiver may terminate this Agreement without prejudice to any rights or remedies if, in the Data Receiver's sole discretion, the Data Receiver concludes that such permissions or consents do not meet applicable Data Protection Laws; and,

4.2.2. the Data Discloser will always, make available, maintain and operate a mechanism for Data Subjects to easily withdraw such permissions and/or consents in accordance with Data Protection Laws.

4.3. **Consent.** If the Data Receiver is relying on the Data Subjects' consent to Process the Controller Personal Information for some or all of the Permitted Purpose, and such consent is being obtained by the Data Discloser on the Data Receiver's behalf:

4.3.1. the Data Discloser warrants that any consent mechanism used to obtain consent from each Data Subject is clear and specific to reasonably ensure that the Data Subject understands the identity of the party or parties to which the Data Subject is consenting to use their Controller Personal Information and the purposes for which such party or parties will use that Controller Personal Information. Without prejudice to the generality of the foregoing, the Data Discloser shall ensure that all such consent mechanisms specifically name the Data Receiver and any third party instructed by the Data Receiver, and the Permitted Purpose for which the Data Receiver is Processing the Controller Personal Information in reliance on the Data Subjects' consent;

4.3.2. the Data Discloser shall maintain a record of all such consents, including the time and date on which consent was obtained, the information presented to Data Subjects in connection with their giving consent, and details of the mechanism used to obtain consent. Data Discloser shall make the aforementioned records available to Data Receiver promptly upon written request;

4.3.3. the Data Discloser shall notify the Data Recipient promptly of any Data Subject who withdraws their consent; and,

4.3.4. the Data Discloser will make available to the Data Receiver, for the Data Receiver's review prior to its use, all such consents mechanisms. The Data Receiver may terminate this Agreement without prejudice to any rights or remedies if, in the Data Receiver's sole discretion, the Data Receiver concludes that such consent mechanism does not meet applicable Data Protection Laws.

4.4. **Retention.** The Data Receiver shall not retain or process the Controller Personal Information for longer than is necessary to carry out the Permitted Purpose or to comply with any statutory or professional retention periods applicable to the Data Receiver.

5. Cooperation

5.1. **Data Subjects' Rights.** Each Party shall, on request by the other Party, provide all reasonable and timely assistance (at their own expense) to enable the other Party to comply with its obligations under Data Protection Laws, specifically in order to enable the other Party to respond to: (i) any request from a Data Subject to exercise any rights under Data Protection Laws in relation to the Controller Personal Information; and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the processing of the Controller Personal Information.

5.2. **Security Incidents and Data Breaches.** If required by Data Protection Laws, if a Party suffers a security incident or Personal Data Breach affecting the Controller Personal Information, it shall notify the other

Party and provide accurate and comprehensive information about the matter in accordance with Data Protection Law. Each Party shall, at the request of the other Party, provide all reasonable assistance in relation to the other Party's obligations under Data Protection Laws to report or notify a security incident or Personal Data Breach involving the Controller Personal Information. The Parties shall comply with any time frames and disclosure requirements as set out in Data Protection Laws (if applicable).

6. Records and Audits

6.1. Each Party shall maintain complete, accurate and up to date written records of all Processing activities carried out on the Data in connection with this Agreement and shall make available to the other Party ("**Requesting Party**"), on written request, such records and any other information as is reasonably required by the Requesting Party to demonstrate the other Party's compliance with its obligations under this Agreement.

6.2. The Requesting Party shall have the right to terminate this Agreement without notice if it considers, acting reasonably, that the other Party is not Processing the Data in accordance with this Agreement.

7. Cross Border Transfers of Data

7.1. If Data originating from the EEA, UK or Switzerland is transferred between the Parties as part of this Agreement and/or the Contract, the relevant module of the EU Standard Contractual Clauses is hereby incorporated into this Agreement and shall apply to the respective Data Exporter and Data Importer as the circumstances require.

7.2. With respect to Data originating from Switzerland, the EU Standard Contractual Clauses shall be amended as follows: (i) references to the term "Member State" shall be substituted for the term "Switzerland" to preserve the rights of data subjects under the Swiss DPA; (ii) references to "Regulation (EU) 2016/679" or "that Regulation" will be understood as references to the Swiss DPA; (iii) the governing law will be the law of the relevant canton; (iv) the competent authority shall be the Swiss Federal Data Protection and Information Commissioner or, where applicable, the competent Cantonal Data Protection Commissioner; and (v) the footnotes shall be removed.

7.3. With respect to Data originating from the UK, the EU Standard Contractual Clauses shall be amended in accordance with the UK Addendum.

7.4. With respect to Data originating from India, the Parties shall not transfer 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 Data is subject to contractual obligations on the recipient that are functionally equivalent to those under this Agreement and the DPDPA.

7.5. With respect to Data originating from the United States, the Parties shall ensure not to transfer, sell, or grant access to any such Data 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").

8. Complying with Data Protections Laws

8.1. Each Party shall in all cases Process the Data in compliance with and shall be individually and separately responsible for complying with, their respective obligations under the Data Protection Laws.

8.2. If any of the Data Protection Laws in any country to which this Agreement relates conflict, the requirements of the country that necessitates stricter or additional requirements to protect Data Subjects' privacy and Data shall be applied.

8.3. Neither Party shall cause the other Party, by act or omission, to be in breach of Data Protection Laws.

9. Liability; Indemnification

9.1. **No Limit on Liability.** Neither Party excludes or limits its liability for: (a) fraud or fraudulent misrepresentation; (b) death or personal injury caused by its negligence; or (c) any matter for which it would be unlawful for the Party to exclude liability.

9.2. **Exclusion of Certain Damages**. Notwithstanding and expressly modifying or taking precedence over anything to the contrary in any other agreements between the Parties, neither Party nor its affiliates, licensors, officers, directors, agencies, employees or representatives shall be liable to the other Party or its affiliates, licensors, officers, directors, agencies, employees or representatives under or in connection with this Agreement for indirect, special, incidental, consequential, or punitive damages or penalties (including, without limitation, lost profits, lost business, business interruption, and the like), however it arises, whether for breach of contract or in tort (including negligence), even if a Party has been advised of the possibility of such damages. This Clause shall not be construed to limit the types of claims for which an indemnity is owed.

9.3. **Indemnity**. Company A agrees to indemnify, keep indemnified and defend at its own expense Company B for all losses, costs, claims, damages and expenses directly incurred by Company B because of failure by Company A to comply with any of its obligations under this Agreement and/or Data Protection Laws.

9.4. 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 Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is subject to the limitations and exclusions of liability in the Contract, 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 Contract and the Agreement together.

10. General Terms

10.1. This Agreement 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.

10.2. Both Parties acknowledge and understand that the Data may be subject to Data Protection Laws that require certain undertakings and/or the entering into of additional agreements, including in relation to the cross-border transfers of the Data. Both parties agree that they shall work together in good faith to 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 Data.

10.3. In the event of any conflict between the provisions of this Agreement, the Contract (if any) and the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail, then this Agreement, then the Contract.

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

10.5. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement 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.

10.6. Any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with this Agreement shall be governed by the laws set out in the Contract (if a Contract exists) otherwise they shall be governed by the law of England and Wales.

10.7. Any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with this Agreement shall be resolved by the courts in the territory set out in the Contract (if a Contract exists) otherwise the courts of England shall have jurisdiction.

Schedule 1:
Description of Processing for Controller Personal Information

1. **Data Subjects**:

☒ Data Discloser's employees, contractors or other personnel

☒ Data Discloser's end users and/or customers

☒ Prospective customers for the Data Receiver

2. **Types of Controller Personal Information**:

☒ Name

☒ Contact details

☒ Other: (please specify) Account usage and related information, including transaction history

3. **Permitted Purpose(s):**

☒ As contemplated by the Contract

☒ Using the Controller Personal Information for sales, marketing and direct marketing purposes, such as sending marketing communications to the Data Subjects

☒ Disclosing the Controller Personal Information to Data Receiver's third party partners or affiliates for their sales, marketing and direct marketing purposes, such as sending marketing communications to Data Subjects

VONTIER™

Schedule 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/execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and act on new information to identify vulnerabilities, remediate, and minimize the 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 critical or controlled 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: •security, confidentiality and integrity of personal data •protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud •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.

Schedule 3:

EU Standard Contractual Clauses

The 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.