Acumatica, Inc.

SCHEDULE 2

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is incorporated into the Subscription SaaS Agreement ("Agreement") between Subscriber and Acumatica, Inc. ("Acumatica"). All defined terms in the Agreement are incorporated by reference. This DPA reflects the parties' agreement with respect to the Processing of Personal Data (as defined below) in connection with the requirements of Data Protection Laws. This DPA will control with respect to the subject matter herein in the event of any conflict with the Agreement. This DPA includes the Standard Contractual Clauses, which are included below.

Definitions. In addition to the definitions in the Agreement and set forth in other sections of this DPA:

"Data Controller" means the entity that determines the purposes and means of Processing Personal Data, in this case, Subscriber.

"**Data Exporter**" means Subscriber or its Affiliate who transfers the Personal Data out of the EEA, Switzerland or the United Kingdom;

"**Data Importer**" means Acumatica or its Affiliate who receives Data from the EEA, Switzerland or the United Kingdom;

"Data Processor" means the entity that Processes Personal Data on behalf of the Data Controller, in this case, Acumatica.

"Data Protection Laws" means any applicable data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including the applicable laws and regulations of the European Union, the European Economic Area and their member states, the United Kingdom and Switzerland.

"Data Subject" means the individual to whom Personal Data relates.

"**EEA**" means the European Economic Area as constituted at the time of the transfer.

"**Model Clauses**" means the standard contractual clauses for the transfer of Personal Data to Processors established in third countries, pursuant to the European Commission Decision C(2010)593, as may be amended or replaced by the European Commission (or in the case of transfers from the United Kingdom, by the competent United Kingdom authority) from time to time.

"Personal Data" means any information relating to an identifiable or identified individual that is provided by Subscriber for "Processing" (defined below) by Acumatica.

"Processing," "Processes," or **"Process"** means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation, or alteration, retrieval, consultation, use, disclosure, dissemination, erasure, or destruction.

"Sub-processor" means any third-party service providers that Process Subscriber Data for Acumatica.

Processing of Personal Data. Subscriber controls the categories of Data Subjects and any Personal Data Processed under this Agreement. Acumatica has no knowledge of, or control over, the Personal Data that Subscriber provides for Processing. Subscriber is solely responsible for the accuracy, quality, and legality of the Subscriber Data and the means by which it acquired the Subscriber Data. Subscriber is solely responsible to ensure that its submission of Personal Data to Acumatica and instructions for the Processing of Personal Data will comply with Data Protection Laws. Acumatica will inform Subscriber without delay if, in Acumatica's opinion, Subscriber's instructions violate Data Protection Laws.

Acumatica will Process Personal Data on behalf of and in accordance with Subscriber's documented instructions (i) in accordance with the Agreement (including all documents incorporated into the Agreement) and (ii) to comply with Subscriber's other reasonable instructions communicated to Acumatica to the extent those instructions are consistent with the Agreement. Apart from such Processing, Acumatica will not Process Personal Data to or for third parties unless required to do so by applicable law; if such a requirement arises Acumatica will make reasonable efforts to inform Subscriber in advance of the required Processing, unless such notice is prohibited by law.

Data Subject Requests. Acumatica shall, to the extent legally permitted, promptly notify Subscriber if Acumatica receives a request from a Data Subject to exercise the Data Subject's right of access, right of rectification, restriction of Processing, right of erasure ("right to be forgotten"), data portability, objection to Processing, or its right not to be Subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Acumatica shall assist Subscriber by appropriate technical and organizational measures, to assist Subscriber in the fulfillment of its obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Subscriber does not have the ability to address a Data Subject Request because it does not have custody or control of the necessary information technology systems, Acumatica shall provide commercially reasonable assistance to facilitate the Data Subject Request, to the extent Acumatica has custody or control of relevant information technology systems and provided that the Data Subject Request is exercised in accordance with Data Protection Laws. To the extent legally permitted, Subscriber shall be responsible and will indemnify Acumatica for any costs arising from Acumatica providing such assistance.

Acumatica Personnel and Sub-processors. Acumatica shall ensure its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements that will survive the termination of their relationship with Acumatica. Acumatica shall ensure that access to Personal Data is limited to those personnel who require access to perform services or Process Personal Data in accordance with the Agreement. Subject to compliance with this paragraph, Subscriber expressly authorizes Acumatica to use Sub-processors to perform specific services on Acumatica's behalf to enable it to perform its obligations under the Agreement. Acumatica has entered into written agreements with its Sub-processors that contain obligations substantially similar to Acumatica's obligations under this DPA and those obligations contained in the Agreement relating to the processing of Personal Data. Acumatica's Sub-processors are::

- Amazon Web Services;
- Microsoft Azure; and
- Any other Acumatica Affiliates

Acumatica will notify Subscriber in writing of changes to its Sub-processors (including new Sub-processors) at least thirty (30) days in advance. If within thirty (30) days of receipt of such notice, Subscriber objects, in writing, to Acumatica's appointment of a new Sub-processor, provided that such objection is based on reasonable grounds relating to data protection, the parties will discuss such concerns in good faith with a goal of achieving resolution, failing which Subscriber may terminate the Agreement and this DPA without further liability upon written notice to Acumatica. Upon request, Acumatica will provide an up to date list of: (i) all Sub-processors involved in processing of Personal Data; (ii) the purposes for which the Sub-processors process Personal Data; and (iii) where the Sub-processors are located. Acumatica will be directly responsible to Subscriber for the acts and omissions of its Sub-processors in relation to the Personal Data.

Security. Acumatica shall maintain appropriate technical and organizational safeguards to protect the confidentiality, integrity, and security of Subscriber Data, including protection from unauthorized or unlawful Processing, accidental or unlawful destruction, unauthorized disclosure or access, accidental loss or alteration, or damage. Acumatica shall notify Subscriber without undue delay (and in any event within 24 hours) after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized access, or unauthorized disclosure of Subscriber Data, including Personal Data, transmitted, stored, or otherwise Processed by Acumatica or its Sub-processor of which Acumatica becomes aware ("Subscriber Data Incident"). Acumatica shall make reasonable efforts to identify the cause of such Subscriber Data Incidents and take steps it deems necessary and reasonable to remediate the cause of such incidents to the extent doing so is within Acumatica's control. These obligations do not apply to incidents that are caused by Subscriber, its affiliates, or users.

GDPR. Acumatica will Process Personal Data in accordance with the General Data Protection Regulation ("GDPR")

requirements to the extent applicable. Upon Subscriber's request, Acumatica shall provide Subscriber with reasonable cooperation and assistance to the extent needed for Subscriber to fulfill its obligation under the GDPR to conduct a data protection impact assessment related to Subscriber's use of the Services, but only where Subscriber does not have access to relevant information that is only available from Acumatica. To the extent required by the GDPR, in connection with the tasks in this section, Acumatica will provide reasonable assistance to Subscriber in cooperation, or prior to consultation, with any Supervisory Authority.

Data Transfers. Where Personal Data originating from the EEA, Switzerland and/or the United Kingdom is Processed by Acumatica outside the EEA, Switzerland or the United Kingdom (as applicable) in a territory that has not been designated by the competent EEA, Swiss and/or United Kingdom authority as ensuring an adequate level of protection pursuant to Data Protection Laws, then:

a. the Model Clauses are incorporated into this DPA by this reference, with each Data Exporter and Data Importer being deemed to have entered into the Model Clauses in its own name and on its own behalf as follows: (i) the applicable law for the purposes of clauses 9 and 11.3 of the Model Clauses shall be the law of the country in which the Data Exporter is established; (ii) Appendices 1 and 2 to the Model Clauses are deemed to incorporate the attachments to this DPA; and (iii) the optional illustrative indemnification clause in the Model Clauses are deemed to have been deleted;

b. if there is any conflict between this DPA and the Model Clauses, the Model Clauses will prevail;

c. in the event that the current Model Clauses are superseded or replaced by new standard contractual clauses approved by the competent EEA, Swiss and/or United Kingdom authority for the Personal Data, the Data Exporter and the Data Importer agree that such new standard contractual clauses shall automatically apply to the transfer of Data from the Data Exporter to the Data Importer and shall be deemed completed on a mutatis mutandis basis to the completion of the Model Clauses as described above;

d. If a Data Importer becomes aware that any law enforcement, regulatory, judicial or governmental authority (an "**Authority**") wishes to obtain access to or a copy of some or all Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Personal Data to such Authority, the Data Importer shall: (i) immediately notify the Data Exporter of such Authority's data access request; (ii) inform the Authority that any and all requests or demands for access to Personal Data should be notified to or served upon the Data Exporter (the original data controller) in writing; and (iii) not provide the Authority with access to Personal Data unless and until authorized by the Data Exporter. In the event a Data Importer is under a legal prohibition or a mandatory legal compulsion that prevents them from complying with (i)-(iii) in full, the Data Importer shall use reasonable and lawful efforts to challenge such prohibition or compulsion (and the Data Exporter acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request). If a Data Importer makes a disclosure of Personal Data to an Authority (whether with Data Exporter's authorization or due to a mandatory legal compulsion) the Data Importer shall only disclose such Personal Data to the extent the Data Importer is legally required to do so and in accordance with applicable lawful process.

e. Clause 4(d) shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Personal Data, a Data Importer has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, the Data Importer shall notify the Data Exporter as soon as possible following such Authority's access and provide the Data Exporter with full details of the same, unless and to the extent the Data Importer is legally prohibited from doing so.

f. Each Data Importer shall not knowingly disclose Personal Data to an Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society. Each Data Importer shall have in place, maintain and comply with a policy governing Personal Data access requests from Authorities it shall which at minimum prohibits: (i) massive, disproportionate or indiscriminate disclosure of Personal Data relating to data subjects in the EEA and the United Kingdom; and (ii) disclosure of Personal Data relating to data subjects in the EEA, Switzerland and the United Kingdom to an Authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such Personal Data.

g. Each Data Importer shall have in place and maintain in accordance with good industry practice measures to protect Personal Data from interception (including in transit from Data Exporter to the Data Importer and between different systems and services). This includes having in place and maintaining network protection to deny attackers the ability to intercept Personal Data and encryption of Personal Data whilst in transit to deny attackers the ability to read Personal Data.

Audit. Acumatica shall permit Subscriber (or its appointed third party auditors) to audit Acumatica's compliance with this DPA, and shall make available to Subscriber all information necessary for Subscriber (or its third-party auditors) to conduct such audit. Acumatica acknowledges that Subscriber (or its third-party auditors) may enter its premises for the purposes of conducting this audit, provided that Subscriber gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Acumatica's operations. Subscriber will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) Subscriber believes a further audit is necessary due to a Subscriber Data Incident suffered by Acumatica. In the event that Acumatica is regularly audited against ISO 27001, SSAE 18 SOC 1, 2 and 3, and/or PCI standards, as applicable, by independent third party auditors, Acumatica shall supply a summary copy of its audit report(s) to Subscriber upon request, which reports shall be subject to the confidentiality provisions of the Agreement.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses and must be completed and signed by the Parties.

A. Data exporter

The data exporter is the Subscriber, as defined in the Subscription SaaS Services Agreement ("Agreement").

B. Data importer

The data importer is Acumatica, Inc. ("Acumatica"). Acumatica is a provider of adaptable cloud and browser-based enterprise resource planning software, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

C. Data subjects

The data exporter may submit Personal Data to Acumatica's Service, the extent of which is determined and controlled by the Data Exporter in its sole discretion.

The Personal Data may include, but is not limited to Personal Data concerning the Data Exporter's end users including employees, contractors and the personnel of the Subscriber and its suppliers, collaborators, and subcontractors. Data Subjects also includes individuals attempting to communicate with or transfer personal information to the Data Exporter's end users.

D. Categories of data

The Data Exporter may submit Personal Data to the Acumatica Service, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Professional skills information
- Personal life data
- Employee compensation information
- Connection data
- Localisation data
- Website usage information
- Email data
- System usage data
- Application integration data
- Other electronic data submitted, stored, sent, or received by end users via the Acumatica Service

E. Special categories of data (if appropriate)

The Data Exporter may submit special categories of Personal Data to the Acumatica Service, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of sensitive Personal Data:

- Health and medical information
- Other electronic sensitive data submitted, stored, sent, or received by end users via the Acumatica Service

F. Processing operations

The personal data transferred will be subject to the following basic processing activities:

Scope of Processing

Personal data may be processed for the following purposes: to provide the third-level support services to

[Subscriber] for [Subscriber's] end users. The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its sub-processors maintain facilities as necessary for it to provide the Service.

Term of Data Processing

Data processing will be for the term specified in the Agreement. For the term of the Agreement, and for a reasonable period of time after the expiry or termination of the Agreement, the Data Importer will provide the Data Exporter with access to, and the ability to export, the Data Exporter's personal data processed pursuant to the Agreement.

Data Deletion

For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to delete data as detailed in the Agreement.

Access to Data

For the term of the Agreement, the Data Importer will provide the Data Exporter with the ability to access the Data Exporter's personal data from the Service in accordance with the Agreement.

Sub-processors

The Data Importer may engage sub-processors to provide parts of the Service. The Data Importer will ensure sub-processors only access and use the Data Exporter's personal data to provide the Data Importer's products and services and not for any other purpose.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Security Measures

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/ legislation attached):

1. As a "Software as a Service" ("SaaS") provider, Acumatica's approach to information security is a risk management imperative we share with our customers.

2. Our information security program is designed to be consistent with internationally accepted standards and involves a layered, defense-in-depth approach to protecting the confidentiality, integrity and availability of systems and data, deploying administrative, technical and physical controls.

3. Our ERP solutions are designed and developed pursuant to secure software development lifecycle processes, for example, strict control over access to source code, rigorous code review and testing, securely segregated development, test and production environments, etc.

4. We require our entire team to review and certify compliance with a comprehensive set of information security policies, which we then monitor and enforce.

5. We provide regular training to raise awareness regarding cybersecurity and data privacy issues and strive to maintain a corporate culture where employees are vigilant for cyber-threats and prepared for cybersecurity incidents.

6. By hosting our SaaS in Amazon Web Services, we provide our customers with the security benefits that come with the most advanced cloud computing infrastructure on the planet. Aside from the formidable infrastructure security provided by Amazon, Acumatica has architected its services so that customer environments are securely segregated. Administrative access to Acumatica's AWS services is strictly limited to a small number of Acumatica personnel on the basis of "need to know" and "least privilege" and requires the use of Multi-Factor Authentication.

7. These Acumatica employees, as well as those who support customers and may need to access customer databases for support purposes, can only do so through encrypted channels via an Acumatica IP address. This means that Acumatica's access to a customer database for support purposes requires a connection through either an Acumatica physical facility or office or the Acumatica VPN, which uses TLS 1.2 or IPSEC. The data associated with such activity is logged by our security personnel.

8. Customers control access rights and management within their dedicated Acumatica SaaS environment by assigning access credentials and can further delineate access by IP address.

9. Availability of customer data is ensured through a system of redundant backups across AWS regions, daily, weekly, monthly and quarterly. The backups are encrypted as well as regularly tested. Retention of the various backups is scheduled so as to provide for recovery under multiple different scenarios and varying historical timing implications.