**Acumatica, Inc.**

**DATA PROCESSING ADDENDUM**

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the applicable End-User License Agreement or Acumatica Subscription SaaS Agreement (the "**Agreement**") between the Subscriber and Acumatica, Inc. ("**Acumatica**"). This DPA reflects the parties' agreement with respect to the Processing of Personal Data (as defined below) to ensure compliance 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 incorporated by reference below.

**Definitions.** Capitalized terms used herein and not otherwise defined in this DPA shall have the meaning set forth in the Agreement:

**"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 Personal 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 data protection laws and regulations applicable to a party and its respective Processing of Personal Data under the Agreement, including the where applicable GDPR and the Swiss DPA.

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

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

"**GDPR**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); and (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); in each case as may be amended or superseded from time to time;

**"Personal Data"** means any Subscriber Data that is protected as "personal data", "personal information", or the like under Data Protection Laws that is Processed by Acumatica as a Data Processor in connection with the Service.

**"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.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data from Switzerland to any other country which is not determined to provide adequate protection for personal data by the Federal Data Protection and Information Commission or Federal Council (as applicable).

"**Standard Contractual Clauses**" or "**EU SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 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, as amended, superseded or replaced from time to time.

**"Sub-processor"** means any third-party Data Processor that Processes Personal Data for Acumatica.

"**Subscriber"** means the entity procuring the SaaS services under the Agreement.

"**Subscriber Data Incident**" means a confirmed breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed in environments controlled by Acumatica or its Sub-processors.

"**Swiss DPA**" means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).

"**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as amended, superseded or replaced from time to time.

**Processing of Personal Data.** Subscriber controls the categories of Data Subjects and any Personal Data Processed under this Agreement, the details of which are set out in Annex I. Acumatica has no knowledge of, or control over, the specific Personal Data that Subscriber provides for Processing in the course of the Services. Subscriber is solely responsible for: (a) the accuracy, quality, and legality of the Subscriber Data and the means by which it acquired the Subscriber Data; and (b) ensuring that its submission of Personal Data to Acumatica and instructions for the Processing of Personal Data comply with Data Protection Laws. Acumatica is not responsible determining if Subscriber's Processing instructions are compliant with applicable law; however Acumatica will inform Subscriber without delay if, in Acumatica's opinion, Subscriber's instructions violate Data Protection Laws, and Acumatica shall not be required to comply with such instructions. Taking into account the nature of the Processing, Subscriber agrees that it is unlikely that Acumatica would become aware of Personal Data Processed by Acumatica is inaccurate or outdated. To the extent Acumatica becomes aware of such inaccurate or outdated data, Acumatica will inform the Subscriber.

**Processing Instructions**. Acumatica will Process Personal Data on behalf of and in accordance with Subscriber's lawful documented instructions. For these purposes, Subscriber instructs Acumatica to Process Personal Data to (i) perform the Services in accordance with the Agreement (including this DPA and 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 ("**Permitted Purposes**"). The parties agree that the Agreement (including this DPA) sets out Subscriber's complete and final instructions to Acumatica in relation to the Processing of Personal Data and Processing outside the scope of these instructions (if any) shall require prior written agreement between the parties. 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 and where the Subscriber is identified or identifiable from the request, promptly notify Subscriber if Acumatica receives a request from a Data Subject seeking to exercise any of its rights under Data Protection Law in connection with the Processing of Personal Data, including rights of access, rectification, restriction, erasure, data portability, objection ("**Data Subject Request**"). 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 (and Acumatica does) and taking into account the nature of the Processing, Acumatica shall provide Subscriber with commercially reasonable assistance (including by appropriate technical and organizational measures, in so far as is possible) to enable Subscriber to respond to a Data Subject Request. To the extent Subscriber requires any additional assistance, Subscriber shall be responsible and will indemnify Acumatica for any costs arising from Acumatica providing such assistance.

**Acumatica Personnel**. 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, are subject to a duty of confidentiality (whether contractual or statutory) and that they will only Process Personal Data for the Permitted Purposes. 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.

**Sub-processors**. Subject to compliance with this paragraph, Subscriber expressly authorizes Acumatica to use Sub-processors, including the following Sub-processors (the "Sub-processor List"):

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

Acumatica shall ensure that:
(a) Sub-processors shall be bound by a written agreement, including data protection and security measures, no less protective of Personal Data than the Agreement and this DPA; (b) Acumatica shall be liable for any breach of this DPA caused by an act, error or omission of its Sub-processors to the extent Acumatica would have been liable had such breach been caused by Acumatica; and (c) Acumatica will notify Subscriber in writing if it adds a new Sub-processor to the Sub-processor List 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 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 Sub-processor List.

**Security**. Acumatica shall implement and maintain appropriate technical and organizational safeguards designed to protect the confidentiality, integrity, and security of Subscriber Data, including protection from Subscriber Data Incidents, as further described in Annex II of this DPA ("**Security Measures**"). Acumatica may update the Security Measures from time to time, provided that any updates shall not materially diminish the overall security of Subscriber Data. Acumatica shall notify Subscriber without undue delay after becoming aware of 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. To the extent that a Subscriber Data Incident is caused by Subscriber, its affiliates, or users, the Subscriber will be responsible for any costs Acumatica incurred while meeting these Security obligations.

**Data Protection Impact Assessments.**

Upon Subscriber's request, Acumatica shall provide Subscriber with reasonable cooperation and assistance to the extent needed for Subscriber to fulfil its obligations under the GDPR to conduct a data protection impact assessment related to Subscriber's use of the Service, 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.

**Return or deletion of Subscriber Data:** Upon termination or expiry of the Agreement, on Subscriber's written request Acumatica shall delete all Personal Data in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent Acumatica is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which data Acumatica shall securely isolate and protect from any further processing and delete in accordance with its deletion practices, except to the extent required by applicable law.

**Data Transfers.** Where Subscriber makes a Restricted Transfer of Personal Data to Acumatica, then the Standard Contractual Clauses shall be deemed incorporated into and form an integral part of this DPA as follows:

**a.** in relation to Personal Data protected by the EU GDPR, the EU SCCs will be completed as follows:

- Module Two will apply;
- in Clause 7, the optional docking clause will apply;
- in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in the section headed " Sub-processors" above;
- in Clause 11, the optional language will not apply;
- in Clause 17, Option 1 will apply, and the EU SCCs will be governed by [Irish] law;
- in Clause 18(b), disputes shall be resolved before the courts of [Ireland];
- Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Agreement;
- Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Agreement, as updated in accordance with this DPA.

**b.** in relation Personal Data protected by the UK GDPR, the Standard Contractual Clauses:

- shall apply as completed in accordance with paragraph (a) above; and
- shall be deemed amended as specified by the UK Addendum, which shall be deemed executed between the transferring Subscriber and Acumatica, and incorporated into and form an integral part of this DPA. In addition, Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in the DPA (including its Annexes) and Table 4 in Part 1 shall be deemed completed by selecting "importer"; and

any conflict between the terms of the Standard Contractual Clauses and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

**c.** In relation to transfers of Personal Data protected by the Swiss DPA, the Standard Contractual Clauses shall apply completed in accordance with paragraph (a) above with the following modifications:

- references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein;
- references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and "Swiss law" and references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "competent Swiss courts"; and
- the Standard Contractual Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

**d.** If there is any conflict between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

**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 reasonably necessary for Subscriber (or its third-party auditors) to conduct such audit. 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.

## ANNEX 1 - DATA PROCESSING DESCRIPTION

This Annex forms part of the DPA and describes the processing that Acumatica will perform on behalf of the Subscriber.

### A. LIST OF PARTIES

**Controller(s) / Data exporter(s)**:

| | | |
|---|---|---|
| 1. | Name: | Subscriber, as defined in the Subscription SaaS Services Agreement ("Agreement") |
| | Address: | As set out in the Agreement and applicable Order Forms. |
| | Contact person's name, position and contact details: | The administrator contacts registered by the Subscriber when creating an account with Acumatica. |
| | Activities relevant to the data transferred under these Clauses: | Subscriber (data exporter) will use Acumatica's (data importer's) enterprise resourcing planning platform for personnel management purposes. |
| | Signature and date: | This Annex 1 shall be deemed executed upon execution of the Agreement. |
| | Role (controller/processor): | Controller |

**Processor(s) / Data importer(s)**: *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

| | | |
|---|---|---|
| 1. | Name: | Acumatica, Inc. ("Acumatica"). |
| | Address: | 3933 Lake Washington Blvd NE #350, Kirkland, Washington 98033, USA. |
| | Contact person's name, position and contact details: | Acumatica's legal counsel with responsibility for privacy can be contacted at privacy@acumatica.com. |
| | Activities relevant to the data transferred under these Clauses: | Acumatica (data importer) is a provider of a cloud-based enterprise resource planning platform. |
| | Signature and date: | This Annex 1 shall be deemed executed upon execution of the Agreement. |
| | Role (controller/processor): | Processor |

### B. DESCRIPTION OF TRANSFER

| | |
|---|---|
| Categories of data subjects whose personal data is transferred: | The Data Exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the Data Exporter in its sole discretion.<br><br>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 Data to the Data Exporter's end users. |
| Categories of personal data transferred: | 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<br>• Title<br>• Position<br>• Employer<br>• Contact information (company, email, phone, physical business address)<br>• ID data<br>• Professional life data<br>• Professional skills information<br>• Personal life data<br>• Employee compensation information<br>• Connection data<br>• Localisation data<br>• Website usage information<br>• Email data<br>• System usage data<br>• Application integration data<br>• Other electronic data submitted, stored, sent, or received by end users via the Acumatica Service |
| Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: | 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:<br><br>• Health and medical information<br>• Other electronic sensitive data submitted, stored, sent, or received by end users via the Acumatica Service<br><br>Any such special categories of data will be protected in accordance with the measures set out in Annex II. |
| The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): | Continuous for the duration of the Acumatica Service. |
| Nature of the processing: | The provision of the Acumatica Service to Subscriber in accordance with the Agreement. |
| Purpose(s) of the data transfer and further processing: | The Permitted Purposes (as defined in the DPA) shall include Processing or providing support services to the Subscriber for Subscriber's end users. The Data Exporter also 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. |
| The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: | 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, following |

| | |
|---|---|
| | which the Personal Data will be deleted. |
| For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: | The nature and duration of the processing are as set out above and in the Agreement.<br><br>The subject matter of the processing concerns the processing of the Personal Data about the categories of Data Subjects, each as set out in this Annex I. |

## C. COMPETENT SUPERVISORY AUTHORITY

| | |
|---|---|
| Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs) | The competent supervisory authority will be determined in accordance with Clause 13 of these Standard Contractual Clauses. |

**Annex II – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES**

**Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.**

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, and securely segregated development, test, and production environments.

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. 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 to provide recovery under multiple different scenarios and varying historical timing implications.

9. Acumatica uses leading-edge technology to ensure that the person who is trying to access your company's data is exactly who they say they are. For example, user logins can be limited to specific IP addresses, which means that no one without a recognizable IP address will be able to access the system. A variety of password protection measures can be put in place as well. You can decide how often users are prompted to change their passwords. Password complexity requirements can help ensure only difficult-to-crack passwords are chosen. Even one-time password and single-sign-on solutions can be installed, which means a unique multi-factor method of access is required to gain access at every log-in attempt.

10. Acumatica allows customers to control user access to their data, functions, and features that are necessary to the user's role using a role-based access control approach.

11. Acumatica offers data encryption as the main feature. Acumatica uses the same encryption technology that protects financial institutions as well as the United States military. Sensitive fields such as credit card and social security numbers within your SQL databases are encrypted. For internal systems Advanced Encryption Standard (AES) 128, 192, or 256-bit encryption. External access to Acumatica portal is via TLS 1.2.

12. Acumatica has a fully staffed, highly trained, 24/7 security operations center already. It's their responsibility to monitor and protect your data.