

# END USER LICENSE AGREEMENT

## AGENT FLEET BY ACUITY ANALYTICS

---

*AWS Marketplace Edition*

Effective Date: August 18, 2026

Version 1.0

---

**IMPORTANT — PLEASE READ THIS AGREEMENT CAREFULLY BEFORE ACCESSING OR USING THE SERVICE. THIS DOCUMENT CONSTITUTES A LEGALLY BINDING CONTRACT BETWEEN YOU ("CUSTOMER") AND ACUITY KNOWLEDGE PARTNERS (UK) LIMITED. BY CLICKING "ACCEPT," SUBSCRIBING THROUGH AWS MARKETPLACE, OR ACCESSING THE SERVICE, YOU AGREE TO BE BOUND BY ALL TERMS HEREIN. IF YOU DO NOT AGREE, DO NOT ACCESS OR USE THE SERVICE.**

This EULA is supplemental to and incorporates by reference the AWS Marketplace Subscriber Terms of Service. In the event of any conflict between this EULA and the AWS Marketplace Terms, this EULA shall govern with respect to the Service-specific terms set forth herein.

## TABLE OF CONTENTS

|            |                                                      |
|------------|------------------------------------------------------|
| Section 1  | Definitions                                          |
| Section 2  | License Grant & Subscription Rights                  |
| Section 3  | Acceptable Use Policy & Restrictions                 |
| Section 4  | Intellectual Property Ownership                      |
| Section 5  | Data Rights & No-Training Covenant                   |
| Section 6  | Data Protection & Privacy (GDPR / CCPA / State Laws) |
| Section 7  | EU AI Act Compliance Framework                       |
| Section 8  | Confidentiality                                      |
| Section 9  | Warranties & Representations                         |
| Section 10 | Indemnification                                      |
| Section 11 | Limitation of Liability                              |
| Section 12 | Term & Termination                                   |
| Section 13 | AI Governance & Responsible AI                       |
| Section 14 | Security                                             |
| Section 15 | Audit Rights & Compliance Verification               |
| Section 16 | Fees, Payment & AWS Marketplace Billing              |
| Section 17 | Governing Law & Dispute Resolution                   |
| Section 18 | General Provisions                                   |
| Exhibit A  | Data Processing Addendum (DPA)                       |
| Exhibit B  | Acceptable Use Policy (AUP)                          |
| Exhibit C  | Sub-Processor List                                   |
| Exhibit D  | Security Standards & Controls                        |

## **PREAMBLE & ACCEPTANCE**

This End User License Agreement ("EULA" or "Agreement") is entered into between Acuity Knowledge Partners (UK) Limited, (company registration number: 04590033), a company formed under the laws of England and Wales having office at 4<sup>th</sup> Floor, Martin House, 5 Martin Lane, London EC4R 0DP, UK ("Acuity Analytics," "we," "us," or "our"), and the entity or individual ("Customer," "you," or "your") subscribing to Agent Fleet by Acuity Analytics through the AWS Marketplace.

This Agreement governs Customer's access to and use of Agent Fleet by Acuity Analytics, Acuity Analytics' proprietary AI-powered multi-agent research and analytics platform ("Agent Fleet"). The Agreement becomes effective upon the earliest of: (i) Customer clicking "Accept" during the AWS Marketplace subscription process; or (ii) the Effective Date specified in an Order Form referencing this EULA.

**IF CUSTOMER IS ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, CUSTOMER REPRESENTS THAT IT HAS THE AUTHORITY TO BIND SUCH ENTITY TO THIS AGREEMENT. IF CUSTOMER DOES NOT HAVE SUCH AUTHORITY, OR IF CUSTOMER DOES NOT AGREE TO THE TERMS OF THIS AGREEMENT, CUSTOMER MUST NOT ACCESS OR USE THE SERVICE.**

## SECTION 1. DEFINITIONS

As used in this Agreement, the following terms have the meanings set forth below:

**1.1 "Acuity Analytics":** means Acuity Knowledge Partners (UK) Limited, (company registration number: 4590033), a company formed under the laws of England and Wales having office at 4<sup>th</sup> Floor, Martin House, 5 Martin Lane, London EC4R 0DP, UK.

**1.2 "Agent Fleet" / "Service":** means Agent Fleet by Acuity Analytics, Acuity Analytics' proprietary AI-powered agentic workflow and analytics platform, including all its software, agents, APIs, dashboards, documentation, updates, and related functionality made available to Customer as a software-as-a-service offering through AWS Marketplace.

**1.3 "Agent Output" / "Generated Content":** means any text, data, analysis, report, recommendation, code, visualization, or other content generated by the Service in response to Customer Data or Prompts.

**1.4 "Agentic Workflow":** means an automated, multi-step sequence of tasks executed by one or more AI agents within the Service, including the use of tools, retrieval mechanisms, task delegation, workflow orchestration, and iterative decision support processes, whether operating autonomously or with human oversight as configured by the Customer.

**1.5 "Authorized User":** means any natural person employed by or contracted to Customer who is authorized by Customer to access and use the Service under Customer's subscription, subject to the user limits specified in the applicable Order Form.

**1.6 "AWS Marketplace":** means the Amazon Web Services digital catalog through which Customer has subscribed to the Service, located at <https://aws.amazon.com/marketplace>.

**1.7 "Confidential Information":** means all non-public information disclosed by one party to the other in connection with this Agreement, whether oral, written, or electronic, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and circumstances of disclosure. Confidential Information includes, without limitation, Customer Data, Prompts, Agent Outputs, business plans, pricing, and technical specifications.

**1.8 "Controller" / "Business":** has the meaning given in GDPR Article 4(7) and, with respect to CCPA, the meaning of "Business" under California Civil Code Section 1798.140(d), as applicable.

**1.9 "Customer Data":** means all data, files, documents, information, and other content submitted by Customer or Authorized Users to the Service, including Prompts and any data uploaded for processing.

**1.10 "Documentation":** means the technical and user documentation for the Service made available by Acuity Analytics or as otherwise provided to Customer.

**1.11 "Effective Date":** means the date on which Customer first accepts this Agreement as described in the Preamble.

**1.12 "Feedback":** means any suggestions, comments, ideas, or recommendations provided by Customer or Authorized Users to Acuity Analytics regarding the Service.

**1.13 "GPAI Model":** means a General Purpose AI model as defined under EU AI Act Article 3(63), including any large language model or foundation model used to power Agent Fleet.

**1.14 "High-Risk AI System":** has the meaning given under Annex III of the EU AI Act (Regulation (EU) 2024/1689).

**1.15 "Model":** means any artificial intelligence or machine learning model, including large language models, embedding models, and fine-tuned models, used to power or support the Service.

**1.16 "Order Form":** means a written or electronic ordering document that specifies the Service tier, subscription term, number of Authorized Users, and fees, and that incorporates this EULA by reference.

**1.17 "Personal Data" / "Personal Information":** means any information relating to an identified or identifiable natural person, as defined under GDPR Article 4(1), CCPA Section 1798.140(v), or other applicable data protection law.

**1.18 "Processor" / "Service Provider":** has the meaning given in GDPR Article 4(8) and, with respect to CCPA, the meaning of "Service Provider" under California Civil Code Section 1798.140(ag), as applicable.

**1.19 "Prompt":** means any instruction, query, or input submitted by an Authorized User or automated system to the Service to elicit an Agent Output.

**1.20 "Sensitive Data":** means Personal Data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data for identification purposes, health data, sex life or sexual orientation data (as defined in GDPR Article 9), as well as Protected Health Information (PHI) as defined under HIPAA, Cardholder Data (CHD) as defined under PCI DSS, and Social Security Numbers or equivalent government-issued identifiers.

**1.21 "Subscription Term":** means the period during which Customer is authorized to access and use the Service, as specified in the applicable Order Form or AWS Marketplace subscription.

**1.22 "Sub-Processor":** means any third-party processor engaged by Acuity Analytics to process Customer Data in connection with the Service, as listed in Exhibit C.

**1.23 "Security Incident":** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

## **SECTION 2. LICENSE GRANT & SUBSCRIPTION RIGHTS**

### **2.1 Grant of License**

Subject to Customer's compliance with this Agreement and timely payment of all applicable fees through AWS Marketplace, Acuity Analytics hereby grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable license during the Subscription Term to: (a) access and use the Service solely for Customer's internal business purposes; (b) permit Authorized Users to access and use the Service in accordance with this Agreement; and (c) access and use the Documentation in support of Customer's authorized use of the Service.

### **2.2 AWS Marketplace Nexus**

The license granted herein is conditioned upon Customer maintaining an active, valid subscription to the Service through AWS Marketplace, including through any AWS Marketplace Private Offer.

Cancellation or termination of Customer's AWS Marketplace subscription automatically terminates the license granted under this Section 2.1, subject to Section 12 (Term & Termination). Suspension of Customer's AWS Marketplace shall correspondingly suspend the license granted under this Section 2.1 for the duration of such suspension, without terminating this Agreement. All fees for the Service must be paid exclusively through AWS Marketplace billing mechanisms, except for fees payable under an enterprise Order Form executed outside AWS Marketplace as contemplated by Section 1.16 and Section 16. Except as set forth in the preceding sentence, no secondary billing arrangements outside AWS Marketplace are permitted.

### **2.3 Authorized Users**

Customer may permit Authorized Users to access the Service up to the user limit specified in the applicable Order Form or AWS Marketplace subscription tier. Customer is responsible for: (a) ensuring all Authorized Users comply with this Agreement; (b) provisioning and de-provisioning Authorized User access; (c) maintaining the confidentiality of all Authorized User credentials; and (d) all acts and omissions of Authorized Users as if they were Customer's own acts and omissions.

### **2.4 Reservation of Rights**

Except for the limited license expressly granted in Section 2.1, Acuity Analytics reserves all rights, title, and interest in and to the Service, including all intellectual property rights therein. No implied licenses are granted under this Agreement.

### **2.5 Beta Features**

Acuity Analytics may make beta, preview, or early-access features of the Service available to Customer from time to time. Such features are provided "as-is" without warranty of any kind and may be discontinued at any time. Acuity Analytics expressly disclaims all liability arising from Customer's use of beta features to the maximum extent permitted by law.

## **SECTION 3. ACCEPTABLE USE POLICY & RESTRICTIONS**

### **3.1 Permitted Use**

Customer may use the Service solely for lawful internal business purposes in accordance with this Agreement, the Documentation, and all applicable laws and regulations.

### **3.2 Prohibited Uses**

Customer shall not, and shall ensure that Authorized Users do not, use the Service to:

- (a) Develop, deploy, or operate weapons systems, military applications, or any technology intended to cause physical harm or death;
- (b) Conduct unauthorized surveillance, tracking, or monitoring of individuals without their knowledge and lawful consent;

- (c) Build or operate discriminatory AI systems for employment decisions, credit scoring, housing allocation, or insurance underwriting in violation of applicable anti-discrimination law;
- (d) Generate, distribute, or facilitate child sexual abuse material (CSAM) or any non-consensual intimate imagery;
- (e) Create deepfakes, synthetic media, or impersonation content intended to deceive, defraud, or harass any individual;
- (f) Conduct cyberattacks, generate malware, exploit software vulnerabilities, or circumvent security controls of any system;
- (g) Engage in social scoring, behavioral manipulation exploiting unconscious biases, or any practice prohibited under EU AI Act Article 5;
- (h) Reverse engineer, decompile, disassemble, or attempt to derive source code or model weights from the Service;
- (i) Resell, sublicense, timeshare, or otherwise provide access to the Service to third parties without Acuity Analytics' express written consent;
- (j) Scrape, crawl, or extract data from the Service in a manner that exceeds normal API usage or circumvents rate limits;
- (k) Use the Service to train, fine-tune, or develop competing AI models or platforms;
- (l) Process Sensitive Data without the express written authorization of Acuity Analytics as described in Section 6.5;
- (m) Use the Service in any manner that violates applicable export control laws, trade sanctions, or embargo regulations;
- (n) Make autonomous, irreversible high-stakes decisions (including medical diagnoses, legal determinations, or financial advice to end consumers) without appropriate human oversight as required by EU AI Act Article 14;
- (o) Provide, distribute, or make available Agent Outputs to any third party as, or as part of, legal, medical, financial, tax, investment, or other regulated professional advice, or as a regulated financial or investment product or service, without the review and supervision of Customer's own appropriately licensed or qualified professionals and in compliance with all professional-responsibility, licensing, and sector-specific regulatory obligations applicable to Customer; or
- (p) Use the Service in connection with any unlawful purpose or in violation of any applicable federal, state, local, or international law or regulation.

### 3.3 Customer Responsibility

Customer assumes sole responsibility for: (a) the legality, accuracy, and appropriateness of all Customer Data submitted to the Service; (b) all Prompts and instructions provided to the Service; (c) all uses of Agent Outputs; and (d) ensuring that its use of the Service complies with all applicable laws, including sector-specific regulations applicable to Customer's industry.

### 3.4 Enforcement

Acuity Analytics reserves the right to investigate suspected violations of this Section 3. Acuity Analytics may suspend Customer's or any Authorized User's access to the Service immediately and without prior notice upon discovering or reasonably suspecting a material violation of Section 3.2. Acuity Analytics may terminate this Agreement for a material violation of Section 3.2 in accordance with Section 12.2; provided that Acuity Analytics may terminate immediately and without a cure period where the violation is not reasonably curable or where continued access poses an imminent risk of harm, unlawful activity, or legal liability to Acuity Analytics or any third party. Violations of this Section may be reported to law enforcement authorities, and Acuity Analytics shall make any report required by applicable law, including any mandatory report of child sexual abuse material.

## **SECTION 4. INTELLECTUAL PROPERTY OWNERSHIP**

### **4.1 Acuity Analytics IP**

As between the parties, Acuity Analytics exclusively owns all right, title, and interest in and to: (a) the Service, including all software, source code, object code, algorithms, models, model weights, architectures, and training methodologies; (b) all Documentation; (c) all aggregated, anonymized, and de-identified usage data derived from Customer's use of the Service (subject to Section 5.4); (d) all improvements, enhancements, and derivative works to the Service; and (e) all trademarks, service marks, logos, and trade names associated with Agent Fleet and Acuity Analytics.

### **4.2 Customer IP**

Customer retains all right, title, and interest in and to: (a) all Customer Data; (b) all Prompts submitted by or on behalf of Customer; (c) all pre-existing intellectual property of Customer used in connection with the Service; and (d) all configurations, workflows, and customizations created by Customer using the Service.

### **4.3 Rights in Agent Output**

To the extent any right, title or interest in Agent Outputs vests in Acuity Analytics, Acuity Analytics hereby assigns it to Customer, so that the Customer owns the Agent Outputs generated specifically in response to Customer's Prompts and Customer Data. Acuity Analytics makes no representation that Agent Outputs are original, non-infringing, or eligible for copyright or other intellectual property right protection under applicable law, including pursuant to U.S. Copyright Office guidance on AI-generated content. Customer is solely responsible for evaluating the Agent Outputs and determining the legal status prior to any use, including any commercial use.

### **4.4 Feedback License**

If Customer or any Authorized User provides Feedback to Acuity Analytics, Customer hereby grants Acuity Analytics a perpetual, irrevocable, worldwide, royalty-free, fully paid-up, sublicensable license to use, reproduce, modify, and incorporate such Feedback into the Service or other products or services, without restriction or compensation to Customer. Acuity Analytics' use of Feedback does not constitute a waiver of any other rights under this Agreement.

#### **4.5 No Implied Licenses**

Nothing in this Agreement grants Customer any license to Acuity Analytics' proprietary AI models, training data, or underlying algorithms beyond the right to receive Agent Outputs as contemplated herein. Customer shall not file any patent application claiming inventions that are based on or incorporate Acuity Analytics' proprietary technology.

### **SECTION 5. DATA RIGHTS & NO-TRAINING COVENANT**

#### **5.1 License to Customer Data**

Customer grants Acuity Analytics a limited, non-exclusive, worldwide license to access, store, process, and use Customer Data solely to: (a) provide the Service to Customer during the Subscription Term; (b) perform maintenance, support, and security operations necessary to deliver the Service; and (c) comply with legal obligations. This license terminates upon expiration or termination of this Agreement, subject to Section 12.

#### **5.2 No-Training Covenant**

**ACUITY ANALYTICS SHALL NOT USE CUSTOMER DATA, PROMPTS, OR AGENT OUTPUTS TO TRAIN, FINE-TUNE, DISTILL, OR OTHERWISE IMPROVE ANY AI MODEL WHATSOEVER, WHETHER OR NOT USED TO POWER THE SERVICE, WITHOUT CUSTOMER'S EXPRESS, AFFIRMATIVE, WRITTEN CONSENT OBTAINED PRIOR TO ANY SUCH USE. THIS PROHIBITION APPLIES TO ACUITY ANALYTICS, ITS AFFILIATES, AND ALL SUB-PROCESSORS.**

#### **5.3 Opt-In Consent for Data Use Expansion**

If Acuity Analytics wishes to use Customer Data for any purpose beyond those specified in Section 5.1, including model training with Customer consent, Acuity Analytics shall: (a) provide Customer with at least 30 days' prior written notice describing the proposed use; (b) obtain Customer's affirmative opt-in consent (not opt-out); and (c) allow Customer to revoke consent at any time with immediate effect. Revocation of consent applies prospectively: upon revocation, Acuity Analytics shall cease all further use of Customer Data for the consented purpose but is not required to reverse or unwind any processing or model training lawfully performed while consent was in effect.

#### **5.4 Aggregated & Anonymized Data**

Notwithstanding Section 5.2, Acuity Analytics may collect, generate, and use aggregated, statistical and de-identified operational data derived from the use of the Service including usage metrics, system performance metrics, reliability metrics, security telemetry and error rates solely for the purposes of operating, maintaining, securing, supporting, analyzing, and improving the Service, developing new product features, benchmarking and business analytics.

Acuity Analytics shall ensure that such data is aggregated and de-identified such that it cannot reasonably be used to identify or re-identify any Customer, any Authorized User, or any individual data subject.

For the avoidance of doubt, Acuity Analytics shall not use Customer Data, Prompts, Agent Outputs, or any de-identified derivatives thereof for AI model training, fine-tuning, distillation, or foundation model development except as expressly authorized pursuant to Section 5.3.

Aggregated and de-identified data meeting the requirements of this Section shall not constitute Customer Data or Personal Data under this Agreement.

## **5.5 Data Portability**

Customer may export Customer Data and Agent Outputs from the Service at any time during the Subscription Term using the export functionality described in the Documentation. Acuity Analytics will provide Customer Data in a structured, commonly used, machine-readable format upon request.

# **SECTION 6. DATA PROTECTION & PRIVACY**

## **6.1 Data Processing Addendum**

To the extent that Acuity Analytics processes Personal Data on behalf of Customer in connection with the Service, the parties agree to be bound by the Data Processing Addendum set forth in Exhibit A, which is incorporated herein by reference. In the event of any conflict between this Agreement and the DPA with respect to the processing of Personal Data, the DPA shall govern.

## **6.2 Roles of the Parties**

The parties acknowledge and agree that: (a) with respect to Personal Data contained in Customer Data, Customer is the Controller/Business and Acuity Analytics is the Processor/Service Provider; (b) Customer remains responsible as a controller for establishing a valid legal basis for the processing of Personal Data and obtaining consent of data subjects whose personal data needs to be processed where required under applicable law; and (c) each party shall comply with its respective obligations under applicable data protection law in its capacity as Controller or Processor.

## **6.3 GDPR Compliance**

Acuity Analytics shall: (a) process Personal Data only on documented instructions from Customer (this Agreement constituting such instructions); (b) ensure that persons authorized to process Personal Data are bound by appropriate confidentiality obligations; (c) implement technical and organizational measures as described in Exhibit D; (d) assist Customer in fulfilling data subject rights requests under GDPR Articles 15–22; (e) notify Customer of any Personal Data breach without undue delay and no later than 72 hours of becoming aware; (f) support Customer in conducting Data Protection Impact Assessments; and (g) delete or return all Personal Data upon termination as described in Section 12.4.

## **6.4 International Data Transfers**

Acuity Analytics shall not transfer Personal Data originating from the European Economic Area, United Kingdom, or Switzerland to any country outside those jurisdictions unless appropriate safeguards are in place, including Standard Contractual Clauses (SCCs) as adopted by the European Commission or equivalent transfer mechanisms. The applicable SCCs are incorporated into Exhibit A.

## **6.5 Sensitive Data**

Customer shall not submit Sensitive Data to the Service unless Customer has obtained Acuity Analytics' express prior written authorization specifying: (a) the categories of Sensitive Data to be processed; (b) the specific processing purposes; and (c) any additional technical and organizational measures required. Acuity Analytics reserves the right to decline to process Sensitive Data or to impose additional requirements as a condition of such authorization.

## **6.6 CCPA / CPRA Compliance**

To the extent Acuity Analytics processes Personal Information of California residents on behalf of Customer: (a) Acuity Analytics acts as Customer's Service Provider and shall not sell, share, retain, use, or disclose such Personal Information for any commercial purpose other than providing the Service; (b) Acuity Analytics shall assist Customer in responding to consumer rights requests under CCPA/CPRA; and (c) Acuity Analytics shall conduct privacy risk assessments to the extent required by applicable California privacy laws and regulations, including CPPA regulations (2025) concerning high-risk processing activities and the use of automated decision-making technologies, where such requirements apply to Acuity's processing activities.

## **6.7 Multi-State Privacy Laws**

Acuity Analytics acknowledges the applicability of comprehensive state privacy laws including, without limitation, the Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Texas Data Privacy and Security Act (TDPSA), and other applicable state laws. The DPA in Exhibit A addresses the parties' respective obligations under such laws.

# **SECTION 7. EU AI ACT COMPLIANCE FRAMEWORK**

## **7.1 Applicability**

This Section 7 applies to the extent that Customer or Authorized Users are located in the European Union or use the Service in connection with activities directed at persons in the European Union. The EU AI Act (Regulation (EU) 2024/1689) applies on a phased manner, and each obligation under the EU AI Act applies from the date on which it becomes applicable under the Regulation, as amended or supplemented from time to time. Each party shall comply with each such obligation as and when it becomes applicable to that party.

## **7.2 Risk Classification**

Acuity Analytics shall maintain and make available upon Customer's reasonable request technical documentation describing Agent Fleet's risk classification under the EU AI Act. Acuity Analytics shall notify Customer in writing within 30 days if Agent Fleet's risk classification changes materially.

## **7.3 Provider Obligations**

To the extent Agent Fleet is subject to provider obligations under applicable AI laws and regulations, including the EU AI Act where applicable, Acuity Analytics shall maintain and implement commercially reasonable measures designed to support compliance with such obligations, including:

- (a) maintaining appropriate quality management and governance processes;

- (b) maintaining technical and operational documentation relating to the Service;
- (c) maintaining logging, auditability, and traceability capabilities sufficient to support investigation, monitoring, and compliance activities;
- (d) providing information reasonably necessary to enable Customer to understand and appropriately use the Service;
- (e) designing and operating Agent Fleet to support effective human oversight, including workflow-based review, validation, approval, escalation, or intervention mechanisms where configured by Customer, required by applicable law, or enabled through the Service; and
- (f) maintaining commercially reasonable measures to promote the accuracy, robustness, resilience, security, and cybersecurity of the Service.

#### **7.4 Deployer Obligations**

As a Deployer of Agent Fleet under the EU AI Act, Customer shall: (a) use Agent Fleet in accordance with the instructions for use provided by Acuity Analytics; (b) implement human oversight measures as specified in Article 14; (c) not make modifications to Agent Fleet that would alter its risk classification; (d) conduct fundamental rights impact assessments where required; and (e) register the deployment in the EU AI Act database where required by Article 49.

#### **7.5 GPAI Model Transparency**

To the extent that Agent Fleet incorporates, accesses, or enables the use of GPAI Models provided by Acuity Analytics or third-party providers, Acuity Analytics shall maintain and make available to Customer, upon reasonable request, documentation describing:

- (a) the GPAI Models made available through the Service, including the identity of the applicable model provider where known;
- (b) the manner in which such GPAI Models are integrated into and utilized by Agent Fleet, including applicable workflow orchestration, agent interactions, governance controls, model-selection processes, and configuration options;
- (c) the human oversight, review, approval, escalation, intervention, auditability, and traceability mechanisms available within the Service;
- (d) material limitations, intended uses, known constraints, and usage restrictions of the Service known to Acuity Analytics or made available by the applicable GPAI Model provider;
- (e) technical documentation, transparency information, compliance disclosures, and copyright-related information regarding such GPAI Models to the extent made available to Acuity Analytics by the applicable GPAI Model provider; and
- (f) documentation and controls designed to support transparency, explainability, auditability, and regulatory compliance within Agent Fleet, including workflow traceability, source attribution where available, agent execution records, audit logs, review checkpoints, and decision-support explanations sufficient to enable users to understand how outputs were generated within the Service.

Customer acknowledges that third-party GPAI Model providers may have independent obligations under applicable laws and regulations, including the EU AI Act, and that Acuity Analytics' obligations under this Section are limited to information and documentation reasonably available to it from such providers.

Acuity Analytics shall not be obligated to provide proprietary model weights, source code, model architectures, training datasets, copyrighted training corpus information, or other information that is not disclosed by the applicable GPAI Model provider.

## **7.6 Prohibited AI Practices**

Neither party shall use Agent Fleet to engage in AI practices prohibited under EU AI Act Article 5 of the EU AI Act, including: (a) AI systems that deploy subliminal techniques to materially distort behaviour in a manner that causes or is likely to cause harm; (b) systems exploiting vulnerabilities of specific groups; (c) social scoring by public authorities; (d) real-time biometric identification in publicly accessible spaces (subject to limited exceptions); or (e) AI systems that infer emotions in workplaces or educational institutions except for safety reasons.

## **7.7 Contractual Requirement**

This Agreement constitutes the written agreement required under EU AI Act Article 25(4) between Acuity Analytics as Provider and Customer as Deployer, establishing the respective responsibilities of each party in connection with the obligations under the EU AI Act.

## **7.8 Transparency of AI-Generated Content**

To the extent Article 50 of the EU AI Act applies, the parties acknowledge that its obligations are allocated according to each party's role. Acuity Analytics, as provider, shall where technically feasible and to the extent required of a provider under Article 50, enable Agent Outputs to be marked in a machine-readable format as artificially generated. Customer, as deployer, is solely responsible for any Article 50 obligation arising from Customer's use, deployment, dissemination, or publication of Agent Outputs, including any obligation to disclose that content is AI-generated or artificially manipulated, to label deepfakes or synthetic content, or to inform natural persons that they are interacting with an AI system. Because Acuity Analytics has no control over and no visibility into how Customer uses Agent Outputs, Customer bears sole responsibility for determining whether Article 50 applies to its use and for fulfilling any resulting obligation.

# **SECTION 8. CONFIDENTIALITY**

## **8.1 Confidentiality Obligations**

Each party ("Receiving Party") agrees to: (a) hold the other party's ("Disclosing Party") Confidential Information in strict confidence using at least the same degree of care as it uses for its own confidential information, but no less than reasonable care; (b) not disclose Confidential Information to any person or entity other than those with a need to know for purposes of this Agreement; and (c) use Confidential

Information solely for purposes of performing its obligations or exercising its rights under this Agreement.

## **8.2 Exceptions**

Confidentiality obligations do not apply to information that: (a) is or becomes publicly available other than through breach of this Agreement; (b) was rightfully known to the Receiving Party prior to disclosure without restriction; (c) is rightfully received from a third party without restriction; or (d) is independently developed by the Receiving Party without reference to the Confidential Information.

## **8.3 Compelled Disclosure**

If a Receiving Party is required by law, regulation, or court order to disclose Confidential Information, the Receiving Party shall: (a) provide the Disclosing Party with prompt written notice (to the extent legally permissible) to enable the Disclosing Party to seek a protective order or other remedy; (b) cooperate with the Disclosing Party in seeking such protection; and (c) disclose only the minimum amount of Confidential Information required by the applicable legal obligation.

## **8.4 AI-Specific Confidentiality Controls**

Acuity Analytics shall implement and maintain commercially reasonable technical, organizational, and administrative safeguards designed to protect Customer's Confidential Information, including Customer Data, Prompts, and Agent Outputs, from unauthorized access, disclosure, alteration, loss, or use.

Such safeguards shall include, as applicable:

- (a)** logical tenant segregation and customer-specific data isolation controls;
- (b)** role-based access controls and authentication mechanisms restricting access to authorized personnel with a legitimate business need;
- (c)** controls designed to prevent Customer Data, Prompts, Agent Outputs, and Confidential Information from being disclosed, surfaced, retrieved, or otherwise made available to other customers through the Service;
- (d)** audit logging and monitoring of access to Customer Data where supported by the Service;
- (e)** encryption and other security measures appropriate to the nature and sensitivity of the information processed; and
- (f)** controls designed to ensure that Customer Data, Prompts, and Agent Outputs are not used for AI model training, fine-tuning, distillation, or model improvement except as expressly permitted under Sections 5.2 and 5.3.

Acuity Analytics shall maintain policies and procedures reasonably designed to support the confidentiality, integrity, and segregation of Customer information throughout the provision of the Service.

## **8.5 Survival**

The obligations of this Section 8 shall survive expiration or termination of this Agreement for a period of five (5) years, except with respect to trade secrets, which shall be maintained in confidence indefinitely.

## **SECTION 9. WARRANTIES & REPRESENTATIONS**

### **9.1 Acuity Analytics Warranties**

Acuity Analytics represents and warrants that:

- (a) the Service will perform materially in accordance with the Documentation during the Subscription Term;
- (b) Acuity Analytics will comply with all applicable laws and regulations in providing the Service;
- (c) Acuity Analytics maintains and will maintain commercially reasonable technical and organizational security measures as described in Exhibit D;
- (d) to Acuity Analytics' knowledge, Agent Fleet does not knowingly infringe the intellectual property rights of any third party (subject to the IP indemnification carve-outs in Section 10.3); and
- (e) Acuity Analytics will fulfill its obligations as a Provider under the EU AI Act as and when those obligations become applicable to Acuity Analytics, including maintaining required technical documentation and logging capabilities to the extent and by the time required under the Regulation.
- (f) Acuity Analytics will use commercially reasonable efforts to ensure that the Service does not contain any viruses, malware, or other malicious code designed to disrupt, disable or harm the Service or Customer's systems. In the event of a breach of this warranty, Acuity Analytics shall, as Customer's sole and exclusive remedy, use commercially reasonable efforts to promptly remediate the affected Service or provide a corrected version.

### **9.2 Customer Warranties**

Customer represents and warrants that:

- (a) Customer has full authority to enter into this Agreement and to bind the entity on whose behalf it acts;
- (b) Customer Data does not and will not infringe the intellectual property rights, privacy rights, or other rights of any third party;
- (c) Customer's use of the Service will comply with all applicable laws and regulations, including sector-specific regulations applicable to Customer's industry;
- (d) Customer has obtained all necessary consents, authorizations, and licenses to submit Customer Data to the Service; and
- (e) Customer will implement appropriate human oversight measures for Agent Outputs used in high-stakes decision-making contexts.
- (f) Customer's Authorized Users will comply with this Agreement, and Customer is responsible for the acts and omissions of its Authorized Users as if they were Customer's own;

- (g) Customer has not submitted and will not submit Sensitive Data to the Service except as expressly authorized by Acuity Analytics under Section 6.5; and
- (h) Customer's use, deployment, and distribution of Agent Outputs will comply with applicable law and will not infringe or violate the intellectual property, privacy, or other rights of any third party.

### **9.3 Disclaimer of Warranties**

EXCEPT AS EXPRESSLY SET FORTH IN SECTION 9.1, THE SERVICE AND ALL AGENT OUTPUTS ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT WARRANTY OF ANY KIND. ACUITY ANALYTICS EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, AND ACCURACY. ACUITY ANALYTICS DOES NOT WARRANT THAT: (A) AGENT OUTPUTS WILL BE ACCURATE, COMPLETE, RELIABLE, OR FREE FROM HALLUCINATIONS OR ERRORS; (B) AGENT OUTPUTS CONSTITUTE LEGAL, MEDICAL, FINANCIAL, OR REGULATORY ADVICE; (C) THE SERVICE WILL BE UNINTERRUPTED, ERROR-FREE, OR SECURE; OR (D) AGENT OUTPUTS WILL BE ELIGIBLE FOR COPYRIGHT PROTECTION UNDER APPLICABLE LAW.

NOTHING IN THIS SECTION 9.3 EXCLUDES, RESTRICTS, OR LIMITS ANY WARRANTY, CONDITION, RIGHT, OR REMEDY TO THE EXTENT THAT IT CANNOT BE EXCLUDED, RESTRICTED, OR LIMITED UNDER APPLICABLE LAW. WHERE APPLICABLE LAW DOES NOT PERMIT THE EXCLUSION OR LIMITATION OF CERTAIN WARRANTIES, THE DISCLAIMERS IN THIS SECTION 9.3 APPLY TO THE MAXIMUM EXTENT PERMITTED BY SUCH LAW.

## **SECTION 10. INDEMNIFICATION**

### **10.1 Indemnification by Acuity Analytics**

Acuity Analytics shall defend, indemnify, and hold harmless Customer and its officers, directors, employees, and agents from and against any third-party claims, damages, losses, and expenses (including reasonable attorneys' fees) arising from: (a) any claim that Agent Fleet, as provided by Acuity Analytics and used in accordance with this Agreement, infringes any third-party patent, copyright, trademark, or trade secret; (b) Acuity Analytics' gross negligence or willful misconduct; (c) Acuity Analytics' material breach of its data protection obligations under Section 6 or Exhibit A; or (d) Acuity Analytics' violation of applicable law in providing the Service.

### **10.2 Indemnification by Customer**

Customer shall defend, indemnify, and hold harmless Acuity Analytics and its officers, directors, employees, and agents from and against any third-party claims, damages, losses, and expenses (including reasonable attorneys' fees) arising from: (a) Customer Data, including any claim that Customer Data infringes or violates the intellectual property, privacy, or other rights of any third-party rights or violates any applicable law; (b) Customer's violation of Section 3 (Acceptable Use Policy); (c) Customer's use, deployment, or distribution of Agent Outputs in a manner that violates third-party rights or applicable law; (d) Customer's unauthorized modification of the Service; or (e) Customer's

breach of any representation or warranty in Section 9.2; or (f) Customer's gross negligence or willful misconduct.

### **10.3 IP Indemnification Carve-Outs**

Acuity Analytics shall have no indemnification obligation under Section 10.1(a) to the extent the claim arises from: (a) Customer's modification of the Service; (b) Customer's use of the Service in combination with products or services not provided or approved by Acuity Analytics; (c) Customer's use of the Service outside the scope of the license granted herein; (d) Customer Data or Prompts submitted by Customer; or (e) Customer's failure to implement updates or patches provided by Acuity Analytics.

### **10.4 Indemnification Procedure**

The indemnified party shall: (a) promptly notify the indemnifying party in writing of any claim for which indemnification is sought; (b) grant the indemnifying party sole control over the defense and settlement of such claim; and (c) provide reasonable cooperation and assistance. The indemnifying party shall not enter into any settlement that imposes liability or obligations on the indemnified party without prior written consent.

### **10.5 IP Remedy**

If the Service becomes or is likely to become subject to an infringement claim under Section 10.1(a), Acuity Analytics may, at its option: (a) procure the right for Customer to continue using the Service; (b) modify the Service to make it non-infringing; or (c) if neither (a) nor (b) is commercially practicable, terminate the Agreement and refund pre-paid fees on a pro-rata basis. The remedies set forth in this Section 10.5, together with the indemnity in Section 10.1 (a), state Acuity Analytics' entire liability and Customer's sole and exclusive remedy for any claim that the Service infringes and third-party intellectual property right.

## **SECTION 11. LIMITATION OF LIABILITY**

### **11.1 Exclusion of Consequential Damages**

**TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF DATA, LOSS OF GOODWILL, OR COST OF SUBSTITUTE SERVICES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE).**

### **11.2 Aggregate Liability Cap**

**TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE TOTAL FEES PAID OR PAYABLE BY CUSTOMER TO ACUITY ANALYTICS (THROUGH AWS MARKETPLACE) DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.**

### **11.3 Enhanced Cap for Data Breaches and Indemnification**

(a) Notwithstanding Section 11.2, Acuity Analytics' aggregate liability for any claims arising from Acuity Analytics' failure of its security obligations under Section 14 or its data protection obligations under Section 6 or Exhibit A shall not exceed two (2) times the total fees paid or payable by Customer during the twelve (12) months preceding the incident. This enhanced cap applies whether such claims are framed as a breach of Section 6, Section 14, Exhibit A, Section 8 (Confidentiality) or otherwise.

(b) Notwithstanding Section 11.2, each party's aggregate liability under its indemnification obligations in Section 10 shall not exceed two (2) times the total fees paid or payable by Customer during the twelve (12) months preceding the event giving rise to the claim.

### **11.4 Exceptions**

The limitations set forth in Sections 11.1 and 11.2 shall not apply to: (a) liability arising from either party's gross negligence or willful misconduct; (b) liability for death or personal injury caused by negligence; (c) liability for fraud or fraudulent misrepresentation; (d) either party's obligations under Section 8 (Confidentiality), except for claims arising from a Security Incident or from a breach of data protection or security obligations affecting Customer Data, which are governed by Section 11.3 (a); (e) Customer's payment obligations under Section 16; or (f) any other liability that cannot be excluded or limited under applicable law. Subject to the foregoing, the limitations and exclusions in this Section 11 apply to the fullest extent permitted by applicable law.

### **11.5 Regulatory Fines**

Each party shall be solely responsible for any regulatory fines, penalties, or assessments imposed on it by any governmental or regulatory authority, including fines under GDPR, UK GDPR, EU AI Act, or other applicable law. Neither party shall be liable under this Agreement for fines or penalties assessed against the other party, except to the extent such fines or penalties are recoverable as part of an indemnified claim under Section 10, in which case they remain subject to the limitations in this Section 11.

### **11.6 Essential Basis**

The parties acknowledge that the limitations of liability in this Section 11 reflect a reasonable allocation of risk between commercial parties and are an essential basis of the bargain and that the fees for the Service reflect this allocation of risk between the parties. Acuity Analytics would not enter into this Agreement without these limitations.

## **SECTION 12. TERM & TERMINATION**

### **12.1 Subscription Term**

This Agreement commences on the Effective Date and continues for the initial Subscription Term specified in the applicable Order Form, AWS Marketplace subscription or AWS Marketplace Private Offer. Unless otherwise specified, in a Order Form or AWS Marketplace Private Offer, the Agreement automatically renews for successive one-year periods unless either party provides written notice of non-renewal at least thirty (30) days prior to the end of the then-current Subscription Term. Where a

AWS Marketplace Private Offer specifies a fixed committed term, the terms of that Private Offer govern renewal, and this Agreement continues for the committed term specified therein.

## **12.2 Termination for Cause**

Either party may terminate this Agreement upon written notice if: (a) the other party commits a material breach of this Agreement and fails to cure such breach within thirty (30) days of receiving written notice specifying the breach; or (b) the other party becomes insolvent, makes a general assignment for the benefit of creditors, or has a receiver, trustee, or liquidator appointed for it or a substantial portion of its assets.

## **12.3 Immediate Termination by Acuity Analytics**

Acuity Analytics may terminate this Agreement or suspend Customer's access immediately and without prior notice if: (a) Customer commits a material violation of Section 3 (Acceptable Use Policy); (b) Customer's use of the Service poses an imminent security risk or legal liability to Acuity Analytics or third parties; (c) Acuity Analytics is required to do so by applicable law, regulatory order, or AWS Marketplace policy; or (d) Customer's AWS Marketplace subscription or AWS Marketplace Private Offer is cancelled, or terminated.

## **12.4 Effect of Termination**

Upon expiration or termination of this Agreement: (a) all licenses granted to Customer under this Agreement immediately terminate; (b) Customer shall immediately cease all use of the Service and delete all copies of the Documentation; (c) Customer may retrieve Customer Data for a period of thirty (30) days following termination using the export functionality described in the Documentation; (d) after such 30-day period and upon written request from the Customer, Acuity Analytics may permanently delete all Customer Data from its systems and shall do so within further thirty (30) days, and will provide written confirmation of deletion upon request; and (e) all outstanding payment obligations remain due and payable, including all fees committed for the remainder of then-current Subscription Term where this Agreement is terminated by Acuity Analytics under Section 12.3 or by reason of Customer's breach.

## **12.5 Survival**

The following Sections survive expiration or termination: Section 1 (Definitions), Section 4 (Intellectual Property), Section 5.2 (No-Training Covenant), Section 8 (Confidentiality), Section 9.3 (Disclaimer), Section 10 (Indemnification), Section 11 (Limitation of Liability), Section 12.4 (Effect of Termination), Section 16.3 (Payment Obligations), Section 17 (Governing Law), and Section 18 (General Provisions).

# **SECTION 13. AI GOVERNANCE & RESPONSIBLE AI**

## **13.1 Human Oversight**

Acuity Analytics shall design and maintain Agent Fleet to enable effective human oversight of AI agent actions. Customer shall implement and maintain human-in-the-loop controls for any high-stakes decision-making processes that rely on Agent Outputs, including but not limited to decisions with significant legal, financial, health, safety, or employment consequences for individuals. Customer

acknowledges that it is solely responsible for the design and operation of such human oversight measures and for any decision made or action taken in reliance on Agent Outputs.

### **13.2 AI Output Disclaimer**

Customer acknowledges and agrees that: (a) Agent Outputs are AI-generated and may contain errors, hallucinations, inaccuracies, or outdated information; (b) Agent Outputs do not constitute legal, medical, financial, regulatory, or professional advice of any kind; (c) Customer is solely responsible for independently reviewing, validating, and verifying Agent Outputs before relying upon them for any business or decision-making purpose; and (d) Acuity Analytics shall not be liable for any decisions made or actions taken by Customer or its Authorized Users based on Agent Outputs without appropriate human review.

### **13.3 Responsible AI Principles**

Acuity Analytics is committed to the following responsible AI principles in developing and operating Agent Fleet: (a) Fairness: testing for and remediating discriminatory outputs and biases; (b) Transparency: disclosing AI involvement in generated content and maintaining explainability; (c) Safety: maintaining content guardrails against harmful outputs; (d) Accountability: maintaining audit trails of agent actions; and (e) Privacy: implementing data minimization and purpose limitation. These principles express Acuity Analytics' internal commitments and aspirations and do not create additional representations, warranties, or contractual obligations beyond those expressly set forth elsewhere in this Agreement.

### **13.4 Agentic Workflow Controls**

With respect to Agentic Workflows, the following requirements apply: (a) all agent actions shall be logged and traceable to the initiating Authorized User; (b) Customer must define and implement authorization boundaries limiting the scope of agent autonomy; (c) Agent Fleet shall not take irreversible external actions (e.g., sending communications, executing financial transactions, deleting data) without explicit human confirmation, unless Customer has expressly configured and authorized such autonomous actions with full knowledge of the risks; and (d) in multi-agent orchestration scenarios, a clear accountability chain must be maintained identifying the responsible Authorized User. Where the Customer configures or authorizes Agent Fleet to take autonomous actions under subsection (c), Customer does so at its own risk and is solely responsible for the consequences of such actions, and Acuity Analytics shall have no liability arising from actions taken within the scope of Customer's configuration and authorization.

### **13.5 AI Transparency Disclosures**

Acuity Analytics shall disclose to Customer: (a) the general nature and capabilities of the AI models used to power Agent Fleet; (b) known material limitations of Agent Fleet; (c) intended use cases and use cases for which Agent Fleet is not designed; and (d) any material changes to the AI models or algorithms that may affect Agent Fleet's outputs, with at least 30 days' prior notice where reasonably practicable.

### **13.6 Accuracy of Product Descriptions**

Acuity Analytics shall use commercially reasonable efforts to ensure that descriptions of Agent Fleet's capabilities in its official marketing materials, AWS Marketplace listing, and Documentation are accurate and not misleading, in all material respects. Customer shall not make representations about Agent Fleet's capabilities to third parties that are inconsistent with the Documentation.

## **SECTION 14. SECURITY**

### **14.1 Acuity Analytics Security Obligations**

Acuity Analytics shall maintain a written information security program, aligned with recognized industry standards (such as ISO 27001 or SOC 2) that includes: (a) encryption of Customer Data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent); (b) role-based access controls and least-privilege principles; (c) multi-factor authentication for administrative access to systems processing Customer Data; (d) regular vulnerability assessments and penetration testing (at least annually); (e) security incident response procedures; and (f) employee security training. Full details are set forth in Exhibit D. Acuity Analytics may update the specific measures from time to time provided that it does not materially reduce the overall level of security during the Subscription Term.

### **14.2 Security Incident Response**

In the event of a Security Incident affecting Customer Data, Acuity Analytics shall: (a) notify Customer without undue delay and no later than 72 hours after becoming aware of the incident; (b) provide a written incident report including the nature of the incident, categories and approximate number of data records affected, likely consequences, and measures taken or proposed; (c) take prompt remedial action to contain and mitigate the incident; and (d) cooperate with Customer in fulfilling Customer's regulatory notification obligations.

### **14.3 Customer Security Obligations**

Customer is responsible for: (a) maintaining the security and confidentiality of all Authorized User credentials; (b) implementing appropriate network-level security for Customer's systems that connect to the Service; (c) promptly notifying Acuity Analytics of any suspected unauthorized access to Customer's account; (d) ensuring Authorized Users do not share credentials; and (e) implementing and maintaining appropriate administrative, technical, physical, and organizational security measures within Customer's environment, including endpoint, network, access, and operational security controls to protect Customer systems and data used in connection with the Service.

### **14.4 AWS Shared Responsibility**

Customer acknowledges that the Service is hosted on AWS infrastructure. The security of the underlying cloud infrastructure is governed by the AWS Shared Responsibility Model. Acuity Analytics is responsible for security of the Service (security in the cloud); AWS is responsible for security of the underlying infrastructure (security of the cloud as defined by AWS); and Customer is responsible for security in the cloud with respect to Customer's own systems and data.

### **14.5 Scheduled Maintenance**

Acuity Analytics may perform scheduled maintenance on the Service from time to time. Acuity Analytics shall use commercially reasonable efforts to: (a) provide Customer with at least five (5) days' prior notice of scheduled maintenance that is reasonably expected to materially affect Customer's use of the Service; (b) conduct such maintenance outside normal business hours where practicable; and (c) minimize any disruption to the availability of the Service. Acuity Analytics may perform emergency maintenance without prior notice where necessary to address a security vulnerability, prevent harm, or preserve the integrity or availability of the Service, and shall notify Customer of such emergency maintenance as soon as reasonably practicable.

## **SECTION 15. AUDIT RIGHTS & COMPLIANCE VERIFICATION**

### **15.1 Records and Recordkeeping**

Acuity Analytics shall maintain complete and accurate records relating to the provision of the Service and its compliance with this Agreement, including EU AI Act technical documentation, for the period specified by Customer's configured retention settings or, where no such settings apply, for a minimum of three (3) years (or such longer period as required by applicable law). Upon Customer's reasonable written request (no more than once per calendar year), Acuity Analytics shall provide Customer with access to such records or, at Acuity Analytics' option, a summary report prepared by an independent auditor.

### **15.2 Third-Party Certifications**

Acuity Analytics shall use commercially reasonable efforts to obtain and maintain relevant third-party certifications, including ISO 27001 and SOC 2 Type II, and shall provide Customer with copies of such certification reports upon request (subject to any confidentiality restrictions imposed by the auditor and to Customer's execution of any confidentiality undertaking reasonably required).

### **15.3 Customer Audit Rights**

Customer may, upon at least thirty (30) days' prior written notice and no more than once per calendar year (unless a material breach is reasonably suspected), inspect Acuity Analytics' records and systems directly relevant to Acuity Analytics' obligations under this Agreement. Any such audit shall be conducted: (a) during normal business hours; (b) in a manner that minimizes disruption to Acuity Analytics' operations; (c) at Customer's sole expense; and (d) subject to Acuity Analytics' reasonable security and confidentiality requirements; and shall not include access to (i) the data or systems of Acuity Analytics' other customers, (ii) Acuity Analytics' proprietary source code, model weights, or algorithms, or (iii) any information the disclosure of which would breach Acuity Analytics' obligations to a third party or applicable law.

### **15.4 Usage Monitoring**

Acuity Analytics may monitor Customer's use of the Service for the purpose of: (a) verifying compliance with usage limits and restrictions under this Agreement; (b) detecting security incidents or AUP violations; and (c) generating aggregated usage statistics. Acuity Analytics shall handle data collected through such monitoring in accordance with its obligations under Section 5 and Section 6.

## **SECTION 16. FEES, PAYMENT & AWS MARKETPLACE BILLING**

### **16.1 AWS Marketplace Billing**

All fees for the Service are billed exclusively through AWS Marketplace, including through any AWS Marketplace Private Offer, in accordance with the subscription tier, AWS Marketplace Private Offer and pricing dimensions selected by Customer. Customer's payment obligations are governed by the AWS Marketplace Subscriber Terms of Service. Acuity Analytics does not process payments directly and is not responsible for AWS Marketplace billing errors or disputes, which must be addressed directly with AWS. The Service is provided solely as a software-as-a-service (SaaS) subscription. Any implementation, consulting, training, integration, or other professional services, if offered by Acuity Analytics shall be provided under a separate written agreement and are not included in, or bundled with, the Service or the fees payable for the Service under this Agreement.

### **16.2 Subscription Tiers & Pricing**

The Service is offered on a subscription basis through AWS Marketplace. Pricing dimensions, including per-seat fees, consumption-based pricing, Market Data Sources pricing, plugin pricing and enterprise flat-rate pricing, are as specified in the applicable AWS Marketplace product listing, Order Form or AWS Marketplace Private Offer. Pricing for a committed Subscription Term is fixed for that term. Upon each renewal, the fees for the renewal term shall automatically increase by five percent (5%) over the fees for the immediately preceding term, unless the applicable Order Form or AWS Marketplace Private Offer expressly specifies a different renewal uplift.

### **16.3 Taxes**

All fees are exclusive of applicable taxes, including sales tax, use tax, value-added tax (VAT), goods and services tax (GST), and any similar or successor charges. For subscriptions transacted through AWS Marketplace, AWS acts as the seller of record and is responsible for calculating, collecting, and remitting applicable transaction taxes in those jurisdictions where AWS provides such tax services, in accordance with AWS Marketplace policies and the AWS Marketplace Seller and Subscriber terms. Customer is responsible for all applicable transaction taxes, except for taxes based on Acuity Analytics' net income. In jurisdictions where AWS does not calculate, collect, or remit taxes, Customer remains responsible for any applicable taxes, and Customer shall self-assess and remit such taxes where required by applicable law (including under any applicable reverse-charge mechanism).

### **16.4 Suspension for Non-Payment**

Acuity Analytics may suspend Customer's access to the Service if Customer's AWS Marketplace Subscription or AWS Marketplace Private Offer is delinquent or suspended due to non-payment, following ten (10) days' written notice to Customer, without terminating this Agreement.

### **16.5 No Refunds**

All fees paid or payable are non-refundable. Customer's obligation to pay the fees for the full committed Subscription Term is not reduced, waived, or refunded by reason of non-use, under-use, or early cessation of use of the Service. Customer is not entitled to refunds for partial periods of use or unused capacity within a subscription tier.

## **SECTION 17. GOVERNING LAW & DISPUTE RESOLUTION**

### **17.1 Governing Law**

This Agreement and any dispute arising out of or relating to it shall be governed by and construed in accordance with the laws of the State of New York, United States, without regard to its conflict of law principles. The United Nations Convention on Contracts for the International Sale of Goods (CISG) does not apply to this Agreement. The parties submit to the exclusive jurisdiction of the state and federal courts located in New York County, New York, and each party consents to the personal jurisdiction of those courts.

EACH PARTY IRREVOCABLY WAIVES ANY RIGHT TO A TRIAL BY JURY IN ANY ACTION, PROCEEDING, OR COUNTERCLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT.

### **17.2 EU Law Carve-Out**

Notwithstanding Section 17.1, mandatory provisions of EU law, including GDPR and the EU AI Act, shall apply to the parties' respective obligations to the extent required by such mandatory provisions, irrespective of the choice of governing law.

### **17.3 Class Action Waiver**

Each party waives any right to bring or participate in any class action, class arbitration, or collective proceeding in connection with any dispute arising under this Agreement.

### **17.4 Injunctive Relief**

Notwithstanding the dispute resolution procedures, either party may seek immediate injunctive or other equitable relief from any court of competent jurisdiction to prevent irreparable harm, protect Confidential Information, or enforce IP rights, without the requirement to post bond or other security.

## **SECTION 18. GENERAL PROVISIONS**

**18.1 Entire Agreement:** This Agreement, together with all exhibits attached hereto (Exhibits A through D), any applicable Order Forms or AWS Marketplace Private Offer, and the AWS Marketplace Subscriber Terms of Service, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements, representations, and understandings. In the event of any conflict, the following order of precedence applies: (a) the commercial terms expressly set out in an applicable Order Form or AWS Marketplace Private Offer; (b) the Data Processing Addendum (Exhibit A), with respect to the processing of Personal Data; (c) the body of this Agreement and its Exhibits; and (d) the AWS Marketplace Subscriber Terms of Service. Notwithstanding the foregoing, mandatory provisions of applicable law shall prevail as set out in Section 17.

**18.2 Amendments:** Acuity Analytics may update or modify this Agreement by providing Customer with at least thirty (30) days' advance written notice of material changes. Customer's continued use of the Service after the effective date of any amendment constitutes acceptance of the modified Agreement. If Customer does not agree to a material amendment, Customer may decline the

amendment by providing notice of non-renewal in accordance with Section 12.1. terminate this Agreement within the notice period.

**18.3 Severability:** If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, illegal, or unenforceable, such provision shall be modified to the minimum extent necessary to make it enforceable, and the remaining provisions shall continue in full force and effect.

**18.4 Force Majeure:** Neither party shall be liable for any delay or failure to perform its obligations (except payment obligations) due to causes beyond its reasonable control, including acts of God, natural disasters, government actions, pandemic, war, terrorism, internet service disruptions, AWS infrastructure outages, or failures of third-party AI model providers or market data source providers. The affected party shall provide prompt written notice and use reasonable efforts to resume performance.

**18.5 Assignment:** Customer may not assign this Agreement or any rights or obligations hereunder without Acuity Analytics' prior written consent, which shall not be unreasonably withheld. Acuity Analytics may assign this Agreement without consent in connection with a merger, acquisition, corporate reorganization, or sale of substantially all of its assets. Any assignment in violation of this Section is void.

**18.6 No Waiver:** No failure or delay by either party in exercising any right, power, or remedy under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise of any such right, power, or remedy preclude any other or further exercise thereof.

**18.7 Relationship of the Parties:** The parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, agency, employment, or franchise relationship between the parties. Neither party has authority to bind the other.

**18.8 Export Controls:** Each Party warrants to the other Party that it is not, nor is it owned or controlled by directly or indirectly, a person or entity that is (i) on the list of Specially Designated Nationals and Blocked Persons maintained by the Office of Foreign Assets Control of the U.S. Department of the Treasury or the U.K. Consolidated Financial Sanctions List maintained by Her Majesty's Treasury; or (ii) subject to country sanctions imposed by the U.S. Government for any reason, including but not limited to being organized or headquartered in or a governmental entity of a country subject to such sanctions; or (iii) organized or headquartered in any other country to which the export or re-export of U.S.-origin goods or technologies are generally embargoed (any such person or entity, a "Prohibited Entity"). Each Party agrees that it will notify the other Party if these circumstances change. Customer warrants that it does not intend to, and agrees not to, supply or use Acuity Analytics' Service to or for the benefit of any Prohibited Entity. If Acuity Analytics determines that it is prohibited under any applicable law or regulation from providing products or services under this Agreement, in addition to any other rights or remedies Acuity Analytics may have, Acuity Analytics may immediately terminate the Agreement and/or any affected Order Form or AWS Marketplace Private Offer.

**18.9 Notices:** All notices under this Agreement shall be in writing and delivered by: (a) email with confirmed receipt to the addresses on file with AWS Marketplace; (b) overnight courier; or (c) certified mail, return receipt requested. Notices to Acuity Analytics shall be sent to: [legal@acuityanalytics.com](mailto:legal@acuityanalytics.com) and Acuity Knowledge Partners (UK) Limited Attention: Legal, 4<sup>th</sup> Floor, Martin House, 5 Martin Lane, London EC4R 0DP, UK.

**18.10 Electronic Signatures:** The parties agree that electronic signatures (including click-through acceptance on AWS Marketplace) are legally binding and have the same legal effect as original written signatures.

**18.11 Publicity:** Customer grant Acuity Analytics the right to use Customer's name and logo to identify Customer as a customer of Agent Fleet on Acuity Analytics' website, customer lists, and marketing and pitch materials. Any other public reference to Customer, including case studies, press releases, or quotations, requires Customer's prior written consent (which may be by email). Customer agrees to consider in good faith reasonable requests to serve as a reference and to provide references to Acuity Analytics' prospective customers. Either party may withdraw the name-and-logo right on written notice, effective prospectively.

**18.12 Counterparts:** This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument.

**18.13 No Third-Party Beneficiaries:** This Agreement is for the sole benefit of the parties and their permitted successors and assigns. Nothing herein creates any rights in any third party.

**18.14 Headings:** Section headings are for convenience only and shall not affect the interpretation of this Agreement.

**18.15 Language:** This Agreement is written in the English language. In the event of any conflict between this Agreement and any translation, the English language version shall prevail.

## EXHIBIT A

### DATA PROCESSING ADDENDUM (DPA)

**THIS DATA PROCESSING ADDENDUM (“DPA”)** forms part and is incorporated into the Agent Fleet by Acuity Analytics End User License Agreement (“EULA”). Any capitalized terms used but not defined in this DPA shall have the meaning provided in the EULA. To the extent there is any conflict in meaning between any provisions of the EULA and this DPA, the terms and conditions in this DPA shall prevail.

#### Definitions

- (a) **“Controller” / “Business”, “Processor” / “Service Provider”, “Data Subject”, “Sub-Processor”, “Personal Data Breach”, “Supervisory Authority”** all have the meanings given to those terms under Privacy Laws.
- (b) **“Customer Personal Data”** means any Personal Data contained within Customer Data that Customer or its Authorized Users provides or makes available to Acuity Analytics through the use of the Service.
- (c) **“Personal Data”** means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Data includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, “personal data” (as defined in the EU/UK GDPR or other Privacy Laws), and any and all information about an individual’s computer or mobile device or technology usage, including (for example and without limitation) IP address, MAC address, unique device identifiers, unique identifiers set in cookies, and any information passively captured about a person’s online activities, browsing, application or hotspot usage or device location and (iii) for the avoidance of doubt includes Personal Data and Sensitive Personal Data.
- (d) **“Privacy Laws”** means all applicable laws and regulations relating to data protection and privacy and/or the Processing of Personal Data, including, but not limited to, Regulation (EU) 2016/679, the General Data Protection Regulation, (“**EU GDPR**”), the EU GDPR in such form as incorporated into the laws of the United Kingdom by virtue of the European Union (Withdrawal Act) 2018 (“**UK GDPR**”), federal and state privacy laws to the extent they apply to the processing of Personal Data in the United States (“**US Privacy Laws**”), including the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (“**CCPA**”), and any associated implementing legislation and regulations, in each case, as in force and applicable, and as amended, supplemented or replaced from time to time.
- (e) **“Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction.
- (f) **“Sensitive Personal Data”** is a subset of Personal Data, which due to its nature has been classified by law as deserving additional privacy and security protections. Sensitive Personal Data consists of: (i) all government-issued identification numbers, (ii) all financial

account numbers (including payment card information and health insurance numbers), (iii) individual medical records, genetic and biometric information, (iv) user account credentials, such as usernames, passwords, security questions/answers and other password recovery data, and (v) data elements that constitute Special Categories of Data under the GDPR, namely Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- (g) **“Transfer”** means to disclose or otherwise make the Personal Data available to a third party, either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.
- (h) **“Transfer Mechanism”** means the applicable Standard Contractual Clauses approved by the European Commission, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or any successor or replacement transfer mechanism recognized under applicable Privacy Laws.

#### **Terms:**

1. This DPA will take effect from the Effective Date of the EULA.
2. The Parties acknowledge that in respect of Customer Personal Data, Customer is the Controller and Acuity is a Processor Processing Personal Data on behalf of Customer, through the Customer's use of the Service. This DPA is incorporated into, and forms part of, the EULA and establishes the rights and obligations of Acuity and Customer with respect to Customer Personal Data Processed via Agent Fleet.
3. In the event that the Customer acts as a Processor in respect of Customer Personal Data, Customer represents and warrants to Acuity that it is validly authorized by the relevant Controller to enter into the EULA and this DPA and make use of Customer Personal Data.
4. Each party shall comply with the provisions of GDPR and other Privacy Laws applicable to it, as a “Controller” or a “Processor” (as defined in GDPR). Acuity shall comply with the provisions of Privacy Laws applicable to it as a “Processor” as defined in the GDPR.
5. Details of Customer Personal Data Processed by Acuity under the EULA are as follows:
  - (i) **Subject Matter, Nature and Purpose of Processing.** Provision, operation, support, security, monitoring, and improvement of the Acuity Agent Fleet Service as described in the EULA.
  - (ii) **Duration of Processing.** Processing of Customer Personal Data by Acuity shall be continuous for the term of the EULA and in accordance with Acuity's retention obligations under the EULA (except where a statutory exception applies).
  - (iii) **Personal Data in Scope.** Customer Personal Data submitted to, stored in, generated by, or otherwise Processed through the Service by or on behalf of Customer and its Authorized Users, including, as applicable: names and contact information; employment and professional information; account, authentication, and user profile information; customer communications and content; usage, device, log, and telemetry data; information contained in prompts, queries, instructions, files, documents, or other content submitted to the Service; and any other Personal Data that Customer or its Authorized Users elect to submit to the Service. Sensitive Data is excluded unless expressly authorized in accordance with the EULA and this DPA.

- (iv) **Category of Data Subjects.** The categories of Data Subjects whose Personal Data may be Processed through the Service are determined by Customer's use of the Service and may include: Customer's employees, contractors, agents, and Authorized Users; Customer's clients, customers, prospects, and business contacts; individuals whose Personal Data is included in content, documents, datasets, prompts, queries, or other materials submitted to the Service by or on behalf of Customer; and any other individuals about whom Customer or its Authorized Users choose to submit Personal Data to the Service.
6. Customer acknowledges that the categories of Personal Data and Data Subjects Processed through the Service are determined by Customer's use of the Service, including the content, data, prompts, queries, workflows, and instructions submitted by Customer and its Authorized Users.
  7. Acuity shall Process Customer Personal Data only as necessary to provide, secure, maintain, support, and improve the Service, and in accordance with Customer's documented instructions as reflected in the Customer's use of the Service, including any prompts, configurations, workflows, and other actions initiated by Authorized Users.
  8. Customer shall be responsible for: (a) determining whether the Service is appropriate for the Customer Personal Data it submits to the Service; (b) ensuring it has all necessary rights, consents and lawful bases required to submit Customer Personal Data to Acuity for Processing through the Service; (c) complying with Privacy Laws applicable to its use of the Service; (d) the content of Customer Data, prompts, instructions, queries, workflows, and configurations submitted to the Service; (e) providing all required notices to Data Subjects; (f) implementing and maintaining appropriate administrative, technical, and organizational measures within its environment to protect Customer systems, accounts, credentials, and data uses in connection with the Service; and (g) configuring and using the Service in a manner consistent with the EULA and this DPA.
  9. Customer acknowledges that the Service is not intended for the Processing of Sensitive Data. Customer shall not submit Sensitive Data to the Service except as expressly authorized in writing by Acuity pursuant to Section 6.5 of the Terms. Where such authorization is granted, the categories of Sensitive Data, processing purposes and applicable safeguards shall be documented in writing. Customer remains responsible for determining whether the Service is appropriate for the Customer Personal Data submitted to the Service.
  10. Acuity shall treat Customer Personal Data as Customer Confidential Information and shall restrict access to Customer Personal Data to personnel, contractors and Sub-Processors who have a legitimate business need to access such data for purposes of providing, securing, maintaining, supporting, or complying with legal obligations relating to the Service, and who are bound by appropriate confidentiality obligations.
  11. Acuity shall ensure that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations and receive privacy and security training appropriate to their responsibilities. Acuity shall conduct personnel screening measures where appropriate and permitted by applicable law.
  12. Acuity shall not Sell or Share Customer Personal Data or otherwise retain, use, disclose, or Process Customer Personal Data outside of the direct business relationship between the Parties, unless obligated to do otherwise by applicable law or regulation or requests or orders of judicial, governmental or regulatory entities, in which case Acuity will inform Customer of

that legal requirement before such Processing occurs unless legally prohibited from doing so.

13. Where Acuity Transfers Customer Personal Data to a country that has not been the subject of an adequacy decision or other recognized lawful transfer mechanism under applicable Privacy Laws, Acuity shall ensure that such Transfer is subject to appropriate safeguards.
14. To the extent required under applicable Privacy Laws, the parties agree that the applicable Standard Contractual Clauses approved by the European Commission, the UK International Data Transfer Agreement or UK Addendum, or any successor or replacement transfer mechanism recognized under applicable Privacy Laws, are hereby incorporated into and form part of this DPA by reference and shall be deemed executed between the Parties, with such modifications as are necessary to reflect the nature of the Processing under this DPA.
15. Acuity may Transfer Customer Personal Data to its affiliates and Sub-Processors provided such Transfers are made in compliance with applicable Privacy Laws and are subject to a legally recognized transfer mechanism where required.
16. Customer provides a general authorization for Acuity to engage Sub-Processors. Acuity shall maintain a current list of Sub-Processors and shall provide notice of material changes. Customer may object on reasonable data protection grounds within thirty (30) days of notification. If the Parties are unable to resolve the objection within a reasonable period, Customer's sole remedy shall be to cease using the affected portion of the Service or terminate the EULA in accordance with its terms.
17. Acuity will ensure that prior to permitting any Sub-Processor to Process Customer Personal Data, the Sub-Processor has entered into a binding written agreement with Acuity that imposes obligations substantially equivalent to the obligations imposed on Acuity under this DPA. Acuity shall remain responsible for the acts and omissions of its Sub-Processors to the extent required under applicable Privacy Laws.
18. To the extent related to its Processing of Customer Personal Data, Acuity shall provide Customer with reasonable assistance:
  - (i) in complying with any requests received from Data Subjects of Customer Personal Data exercising Data Subject rights under Privacy Laws;
  - (ii) to enable Customer to conduct data protection impact assessments and consultations with (or notifications to) a relevant Supervisory Authority where Customer is required to do so under Privacy Laws;
  - (iii) in complying with Customer's obligation to implement and maintain appropriate technical and organizational security measures to protect Customer Personal Data; and
  - (iv) in complying with Customer's obligation to notify a Personal Data Breach to a Supervisory Authority or to a Data Subject as required under Privacy Laws.

Customer acknowledges that Customer retains primary responsibility for responding to Data Subject requests and that Acuity's assistance obligations are limited to Customer Personal Data that Acuity is reasonably able to identify and process within the Service.

19. Acuity will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of Customer Personal Data. Acuity will notify Customer without undue delay after becoming aware of a confirmed Personal Data Breach affecting Customer Personal Data, provide Customer with details of the Personal Data Breach as required under Privacy Laws and promptly take reasonable steps to mitigate the effects of the Personal Data Breach and prevent recurrence. Acuity shall provide such information as is reasonably available to Acuity at the

time of notification and may supplement such information as additional facts become known. Acuity's notification of a Personal Data Breach shall not constitute an admission of fault or liability.

20. Acuity shall implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, taking into account: (a) the state of the art; (b) implementation costs; (c) the nature, scope, context and purposes of processing; and (d) the risks to individuals. The technical and organizational measures implemented by Acuity are described in Exhibit D, which Acuity may update from time to time provided such updates do not materially diminish the overall security of the Service.
21. Customer acknowledges that the effectiveness of the security measures depends in part on Customer's secure use of the Service, including the management of user access, credentials, prompts, configurations, integrations, and Customer Data submitted to the Service.
22. Acuity shall have implemented and documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing the Service in a timely manner after a disruptive event. Acuity will periodically test and monitor the effectiveness of its business continuity and disaster recovery plans. Upon request by Customer, Acuity will provide a summary of its business continuity and disaster recovery capabilities and testing results, subject to confidentiality and security considerations.
23. Acuity shall maintain commercially reasonable insurance coverage appropriate to the nature and scale of its business operations.
24. Upon request not more than once annually, Acuity shall make available information reasonably necessary to demonstrate compliance with this DPA, which may include relevant third-party audit reports, certifications, questionnaires, or security documentation, subject to confidentiality obligations. Customer audit rights, if any, shall be satisfied through such materials unless otherwise required by applicable law.
25. Upon termination of the Agreement, Customer may export Customer Data during the applicable retrieval period. Following expiration of the retrieval period, Acuity shall delete or de-identify Customer Personal Data, except to the extent retention is required by applicable law, regulatory requirements, legitimate backup processes, or legal hold obligations. Notwithstanding the above, Customer acknowledges that Customer Personal Data may remain in routine backups and disaster recovery systems for a limited period until overwritten in accordance with Acuity's retention practices.
26. Each party's aggregate liability under this DPA shall be subject to the provisions and limitations of liability set forth in the EULA, except where prohibited by applicable law.
27. In the event of any conflict or inconsistency between this DPA and any provision of the EULA with respect to the Processing of Customer Personal Data, this DPA shall prevail and have effect to the extent of the conflict.
28. This DPA shall be governed by and construed in accordance with the governing law provisions set forth in Section 17 of the EULA.

## **EXHIBIT B**

### **ACCEPTABLE USE POLICY (AUP)**

This Acceptable Use Policy ("AUP") supplements the Agreement and governs Customer's and its Authorized Users' access to and use of Agent Fleet. Customer is responsible for ensuring that all Authorized Users comply with this AUP.

#### **B.1 Permitted Use Cases**

Subject to the terms of the Agreement, Customer may use Agent Fleet for legitimate business purposes, including:

- Financial research, investment research, due diligence, valuation support, portfolio monitoring, financial spreading, and investment analysis.
- Corporate strategy, market intelligence, competitive analysis, and business planning.
- Research, drafting, document review, and knowledge management activities, including legal, compliance, regulatory, and risk-management support functions, provided that appropriately qualified personnel review all material outputs before reliance.
- Business intelligence, operational analytics, data aggregation, reporting, and dashboard generation.
- Automated document processing, data extraction, summarization, workflow automation, and report generation.
- Customer support, internal knowledge management, and enterprise productivity enhancement.
- Regulatory compliance support, policy analysis, audit preparation, and documentation assistance.
- Development, testing, configuration, and deployment of Agentic Workflows within Customer's authorized business environment.

#### **B.2 Prohibited Uses**

Customer shall not use, and shall not permit any Authorized User to use, the Service to:

- Violate any applicable law, regulation, court order, sanction, or regulatory requirement.
- Engage in fraud, deception, market manipulation, unlawful surveillance, or other unlawful activities.
- Upload, transmit, store, or process malicious code, viruses, malware, ransomware, or harmful software.
- Infringe, misappropriate, or violate intellectual property, privacy, publicity, confidentiality, or other rights of any person or entity.
- Generate or disseminate unlawful, defamatory, fraudulent, harassing, threatening, hateful, discriminatory, or misleading content.
- Attempt to gain unauthorized access to systems, networks, accounts, data, or environments.
- Interfere with, disrupt, degrade, probe, scan, or test the security of the Service except as expressly authorized.

- Circumvent security controls, usage limits, access restrictions, or technical safeguards implemented by Acuity Analytics.
- Develop, train, fine-tune, benchmark, reverse engineer, extract, replicate, or create competing models, products, or services using the Service except as expressly permitted in writing.
- Use the Service in connection with weapons development, unlawful cyber activity, unlawful surveillance, or activities prohibited by applicable law.

### **B.3 Content Standards**

Customer is responsible for the legality, accuracy, quality, and appropriateness of Customer Data, Prompts, and instructions submitted to the Service.

Customer shall ensure that all Customer Data and Prompts:

- Comply with applicable laws and regulations.
- Are submitted with all necessary rights, permissions, consents, and lawful bases for processing.
- Do not contain malicious code, harmful content, or unauthorized third-party information.
- Do not intentionally include information where use of the Service would violate contractual, fiduciary, regulatory, or professional obligations.
- Are appropriate for a professional business environment.

### **B.4 AI-Specific Use Standards**

When using Agentic Workflows, AI agents, automation features, or autonomous workflows, Customer shall:

- Define appropriate business objectives, permissions, and operational boundaries for agent actions.
- Configure and maintain appropriate human oversight and review controls proportionate to the risk of the use case.
- Review outputs before making material business, financial, legal, regulatory, employment, investment, or customer-impacting decisions.
- Maintain appropriate records, logs, approvals, or audit trails where required by applicable law, regulation, or Customer policy.
- Ensure agent actions remain within Customer-authorized scope, permissions, and governance controls.
- Test and validate workflows before deployment in production environments.
- Monitor workflow performance and promptly investigate unexpected, inaccurate, or anomalous outputs.

### **B.5 High-Risk and Regulated Activities**

Customer acknowledges that AI-generated outputs may contain inaccuracies, omissions, or outdated information and are intended to support human decision-making rather than replace professional judgment.

Unless expressly agreed in writing by Acuity and accompanied by any additional controls, assessments, or contractual terms required by applicable law, the Service is not designed, intended, or marketed for use as a high-risk AI system or as the sole basis for decisions that produce legal effects or similarly significant effects on individuals.

Accordingly, Customer shall not rely exclusively on Agent Outputs for:

- Investment decisions.
- Credit decisions.
- Financial workflow decisions.
- Insurance eligibility determination.
- Employment-related decisions, including recruitment, candidate screening, hiring, promotion, performance evaluation, compensation, disciplinary action, or termination.
- Determinations regarding access to education, vocational training, healthcare, housing, public benefits, or other essential services.
- Legal, judicial, law enforcement, immigration, asylum, or border-control decision-making.
- Any other activity classified as a high-risk AI use case under applicable AI regulations.

Where Customer elects to use the Service in connection with any regulated or high-risk activity, Customer is solely responsible for determining the applicability of specific laws and regulations, and for implementing appropriate human oversight, independent validation, risk assessments, and other legally required controls.

## **B.6 Security and Access Controls**

Customer shall:

- Maintain the confidentiality of account credentials.
- Use appropriate authentication and access controls.
- Promptly notify Acuity Analytics of suspected unauthorized access, misuse, security incidents, or compromised credentials.
- Use the Service only through authorized interfaces and documented integration methods.

## **B.7 Monitoring and Enforcement**

Acuity Analytics may investigate suspected violations of this AUP and may suspend or restrict access to the Service where reasonably necessary to:

- Protect the security, integrity, availability, or operation of the Service;
- Comply with applicable law or regulatory requirements; or
- Prevent unlawful, harmful, fraudulent, or unauthorized activity.

Where reasonably practicable, Acuity Analytics shall provide Customer with notice and an opportunity to remediate any violation prior to suspension.

## EXHIBIT C

### SUB-PROCESSOR LIST

As of the Effective Date, Acuity Analytics engages the following Sub-Processors to process Customer Data in connection with the Service. Acuity Analytics will provide 30 days' notice before engaging any new Sub-Processor.

| Sub-Processor             | Purpose                                | Data Location            | Privacy Policy                                                      |
|---------------------------|----------------------------------------|--------------------------|---------------------------------------------------------------------|
| Amazon Web Services (AWS) | Cloud infrastructure, storage, compute | USA / Multi-region       | <a href="https://aws.amazon.com/privacy">aws.amazon.com/privacy</a> |
| Azure OpenAI Services     | AI model inference for agent responses | USA / Multi-region       | Per model provider policy                                           |
| AWS Bedrock Services      | AI model inference for agent responses | USA / Multi-region       | Per provider policy                                                 |
| Snowflake (optional)      | Data warehousing for enterprise tiers  | Customer-selected region | <a href="https://snowflake.com/privacy">snowflake.com/privacy</a>   |
| Pendo                     | Usage Analytics                        | USA                      | Security and privacy in Pendo – Pendo Help Center                   |
| Endex AI                  | Excel Plugin                           | USA/Europe               | <a href="#">Privacy Policy   Endex</a>                              |

## EXHIBIT D

### SECURITY STANDARDS & CONTROLS

Acuity shall maintain and operate the Service in accordance with commercially reasonable administrative, technical, and organizational safeguards designed to protect Customer Data against unauthorized access, disclosure, alteration, destruction, misuse, or loss.

Acuity has implemented, and shall continue to maintain, the following minimum security standards and controls throughout the term of the Agreement.

#### **D1. Information Security Program**

Acuity shall maintain a documented Information Security Management System ("ISMS") designed to support the confidentiality, integrity, and availability of Customer Data.

Acuity's security program is aligned with recognized industry standards and frameworks, including:

- ISO/IEC 27001 principles for information security management.
- SOC 2 Type II control objectives or equivalent assurance frameworks.
- Applicable privacy and data protection regulations, including GDPR and other applicable laws.

Acuity shall maintain the following:

- ISO/IEC 27001 certification
- SOC2 Type II attestation

#### **D2. Identity and Access Management**

Acuity has implemented access control mechanisms designed to restrict access to Customer Data and Service resources to authorized personnel only.

Acuity shall maintain:

- Role-Based Access Control (RBAC).
- Least-privilege access principles.
- Multi-factor authentication for administrative and privileged accounts.
- Segregation of duties for privileged functions where applicable.
- Periodic review and recertification of access rights.
- Support for enterprise Single Sign-On (SSO) integrations where applicable.

#### **D3. Encryption and Key Management**

Acuity has implemented encryption controls to protect Customer Data during transmission and storage.

Acuity shall:

- Encrypt Customer Data in transit using TLS 1.2 or higher.
- Encrypt Customer Data at rest using AES-256 or an equivalent industry-recognized standard.
- Maintain secure cryptographic key management procedures.

- Restrict access to encryption keys to authorized personnel and systems.

#### **D4. Network Security**

Acuity has implemented network security controls designed to reduce the risk of unauthorized access and network-based attacks.

Acuity shall maintain:

- Network segregation and isolation controls.
- Firewalls and Web Application Firewall (WAF) protections.
- Protection against common web application threats, including OWASP Top 10 vulnerabilities.
- Secure administrative access mechanisms.
- Continuous monitoring of network security events and activities.

#### **D5. Application Security**

Acuity has implemented a Secure Software Development Lifecycle (SSDLC) for the design, development, testing, and deployment of the Service.

Acuity shall maintain security practices including:

- Secure coding standards.
- Static Application Security Testing (SAST).
- Dynamic Application Security Testing (DAST).
- Software Composition Analysis (SCA).
- Vulnerability management processes.
- Remediation processes for identified security vulnerabilities based on risk.

#### **D6. Vulnerability and Patch Management**

Acuity has implemented processes to identify, assess, prioritize, and remediate security vulnerabilities.

Acuity shall:

- Conduct periodic vulnerability assessments.
- Third-party based annual Penetration Testing covering OWASP Top 10 AI risks and OWASP Top 10 web attacks.
- Apply security patches and remediation measures within commercially reasonable timeframes.
- Monitor for newly identified threats and vulnerabilities affecting the Service.

#### **D7. Logging, Monitoring, and Incident Detection**

Acuity has implemented security monitoring and logging capabilities to support threat detection, investigation, and incident response activities.

Acuity shall maintain:

- Security logging and monitoring systems.
- Audit trails for authentication events, administrative activities, and access to Customer Data.
- Security event correlation and alerting capabilities.

- Log retention practices consistent with operational, legal, and regulatory requirements.

#### **D8. Data Segregation and Multi-Tenant Security**

Where the Service is provided using a multi-tenant architecture, Acuity has implemented logical segregation controls designed to protect Customer Data from unauthorized access by other customers.

Acuity shall maintain controls to:

- Segregate Customer Data from other customer environments.
- Restrict access to Customer Data based on authorization requirements.
- Prevent cross-tenant access or data leakage.
- Periodically validate tenant isolation mechanisms.

#### **D9. Artificial Intelligence and Automated Processing Security**

Where the Service utilizes artificial intelligence, machine learning, large language models, retrieval-augmented generation (RAG), automated decision-support systems, or agentic workflows, Acuity has implemented controls designed to support the secure and responsible use of such capabilities.

Acuity shall maintain reasonable safeguards to:

- Restrict unauthorized access to Customer Data, prompts, responses, models, embeddings, retrieval indexes, and generated outputs.
- Protect Customer Data from unauthorized access, disclosure, alteration, or loss throughout AI-assisted processing activities.
- Monitor for anomalous, unauthorized, or potentially malicious activity affecting AI systems, models, agents, tools, and supporting infrastructure.
- Maintain logging, auditability, and traceability of AI-assisted activities and agent actions, where technically feasible and appropriate to the Service.
- Implement controls designed to mitigate AI-specific security risks, including prompt injection, unauthorized data disclosure, model misuse, adversarial manipulation, excessive agent privileges, and other security risks.
- Ensure that Customer Data, prompts, and outputs are not used to train, retrain, or fine-tune foundation models or other machine learning models, except where expressly authorized by Customer.
- Maintain human oversight, review, or approval mechanisms where appropriate to the nature of the functionality provided.
- Maintain governance and change management processes for material model, agent, orchestration, or AI system changes that may affect security, privacy, or service functionality.
- Enforce access controls and source-level permissions for RAG and retrieval capabilities to help ensure that users and AI systems may access only content for which they are authorized.
- Limit retrieval activities to authorized repositories, connected data sources, and content accessible to the requesting user or system.
- Provide source attribution, references, citations, or similar traceability mechanisms where supported by the applicable functionality.

- Maintain controls for agentic AI activities, including authorization, logging, and auditability of agent actions.

**D10. Incident Response**

Acuity has implemented and maintains an Incident Response Program designed to identify, investigate, contain, remediate, and recover from security incidents.

Acuity shall maintain:

- Documented incident response procedures.
- Defined incident escalation processes.
- Incident management roles and responsibilities.
- Customer notification procedures consistent with applicable legal, regulatory, and contractual requirements.

**D11. Business Continuity and Disaster Recovery**

Acuity has implemented business continuity and disaster recovery measures designed to support service resilience and recovery following a disruption.

Acuity shall maintain:

- Business Continuity Plans (BCP).
- Disaster Recovery Plans (DRP).
- Backup and restoration procedures.
- Periodic testing and validation of recovery capabilities.

**D12. Personnel Security**

Acuity has implemented personnel security controls designed to protect Customer Data and Service assets.

Acuity shall:

- Require personnel with access to Customer Data to be bound by confidentiality obligations.
- Conduct personnel screening and verification checks where permitted by applicable law.
- Provide periodic security and privacy awareness training to personnel.

**D13. Third-Party and Sub-Processor Security**

Acuity has implemented third-party risk management processes for service providers and sub-processors that support delivery of the Service.

Acuity shall:

- Assess the security posture of relevant third-party service providers.
- Require appropriate contractual security and confidentiality obligations.
- Maintain oversight of sub-processors involved in processing Customer Data.

**D14. Security Program Evolution**



Acuity may modify, improve, replace, or enhance security controls from time to time to address evolving threats, technology changes, regulatory requirements, customer requirements, or industry best practices.

Any such modifications shall not materially diminish the overall security posture of the Service.

*NOTE: For AWS Marketplace subscriptions, Customer's acceptance of this EULA is effected electronically through the AWS Marketplace subscription process. Physical or electronic signatures on this page are required only for enterprise Order Forms executed outside of AWS Marketplace.*