SUBSCRIPTION AND SERVICES AGREEMENT

This subscription and services agreement (this "**Agreement**") is made by and between Acquia Inc., a Delaware corporation, with a principal place of business at 53 State Street, Boston, MA 02109 ("**Acquia**") and Ordering Activity under GSA Schedule contracts identified in the Order ("**Customer**"). This Agreement shall govern the provision of the Services and shall be effective between Acquia and Customer on the latest date signed below ("**Effective Date**").

1. DEFINITIONS.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes hereof, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Ancillary Programs" means certain enabling software or tools, which Acquia makes available to Customer for download as part of the Subscription Services for purposes of facilitating Customer access to, operation of, and/or use with the Subscription Services. Ancillary Programs do not fall within the meaning of Third Party Tools.

"**AI Features**" means (generative) Artificial Intelligence features provided as part of the Subscription Services, allowing AI Users to insert Input in a text-format by way of a prompt or other Input media as an upload, and formulate a request to the AI Features to generate Output.

"**AI Input**" means any text, images, video, audio, software code, or any other information inserted by the AI User in a prompt or upload with a request to the AI Features to create AI Output based on the AI Input.

"**AI Output**" means the response created by AI Features based on the AI Input and the request of the AI User.

"**AI User**" means any user of the AI Features provided to the Customer.

"**Authorized Contractors**" means independent contractors, licensors, or subcontractors.

"**Customer Applications**" means all software programs, including without limitation Drupal, Node.js, and Magento, that Customer uses on the cloud platform comprising part of the Subscription Services. Subscription Services do not fall within the meaning of Customer Applications.

"**Customer Data**" means all data, records, files, images, graphics, audio, video, photographs, reports, forms and other content and material, in any format, submitted to, stored by, transmitted, or otherwise used by or for Customer within the Subscription Services. Any output (i.e content created by) of Third Party Tools does not fall within the meaning of Customer Data until said output is used with the Subscription Services.

"**Data Center Region**" refers to the geographic region in which the Customer Data is housed.

"Deliverable" means any work product, deliverables, programs, interfaces, modifications, configurations, reports, or documentation developed or delivered in the performance of Professional Services.

"**Documentation**" means Acquia's product guides and other end user documentation for the Subscription Services and Ancillary Programs available online and through the help feature of the Subscription Services, as may be updated by Acquia from time to time to reflect the then-current Subscription Services.

"**Order**" or "**Order Form**" means an ordering document or online order specifying the Services to be provided hereunder that is entered into between Acquia and Customer from time to time, including any addenda and supplements thereto. Customer Affiliates may purchase Services subject to this Agreement by executing Orders hereunder.

"Professional Services" means fee-based migration, implementation, training or consulting services that Acquia performs as described in an Order or SOW, but excluding Support Services.

"**Services**" means the Subscription Services and Professional Services that Customer may purchase under an Order or SOW.

"Statement of Work" or "SOW" means a statement of work entered into and executed by the parties describing Professional Services to be provided by Acquia to Customer.

"Subscription Services" means the cloud platform made available by Acquia to Customer, the software made available by Acquia to Customer online via the applicable customer logins and/or associated Support Services, as ordered by Customer under an Order, as applicable.

"Support Services" means the level of support services purchased by Customer pursuant to an Order.

"Subscription Term" means the term of Subscription Services purchased by Customer which shall commence on the start date specified in the applicable Order and continue for the subscription term specified therein and any renewals thereto.

"**Trial Services**" means any Acquia product, service or functionality that may be made available by Acquia to Customer to try at Customer's option, at no additional charge, and which is designated as "beta," "trial," "non-GA," "pilot," "developer preview," "non-production," "evaluation," or by a similar designation.

"Third Party Tools" means any non-Acquia products or services made available as an accommodation through Acquia's Services.

2. SUBSCRIPTION SERVICES

2.1. Provision of Subscription Services. Acquia will make the Subscription Services available to Customer pursuant to this Agreement, the Documentation, and the relevant Order Form during the Subscription Term, solely for Customer's internal business purposes. Acquia's Affiliates and its Authorized Contractors may perform certain aspects of the Services and access Customer Data and Customer Applications provided that Acquia remain fully liable for same and responsible for ensuring that any of Acquia's obligations under this Agreement performed by its Affiliates and its Authorized Contractors are carried out in accordance with this Agreement. Customer's Affiliates and its Authorized Contractors may access certain aspects of the Services hosted or provided through such Services provided that Customer remain fully liable for same and responsible for ensuring that any of Customer's obligations under this Agreement performed by its Affiliates and its Authorized Contractors are carried out in accordance with this Agreement. Customer's use of the Subscription Services includes the right to access all functionality available in the Subscription Services during the Subscription Term. So long as Acquia does not materially degrade the functionality, as described in the

Documentation, of the Subscription Services during the applicable Subscription Term (i) Acquia may modify the systems and environment used to provide the Subscription Services to reflect changes in technology, industry practices and patterns of system use, and (ii) update the Documentation accordingly. Subsequent updates, upgrades, enhancements to the Subscription Services made generally available to all subscribing customers will be made available to Customer at no additional charge, but the purchase of Subscription Services is not contingent on the delivery of any future functionality or features. New features, functionality or enhancements to the Subscription Services may be marketed separately by Acquia and may require the payment of additional fees. Acquia will determine, in its sole discretion, whether access to such new features, functionality or enhancements will require an additional fee.

2.2 Trial Services. If Customer registers or accepts an invitation for Trial Services, including through Acquia's website, or executes an Order for the same, Acquia will make such Trial Services available to Customer on a trial basis, free of charge, until the earlier of (a) the end of the free trial period for which Customer registered to use the applicable Trial Services, or (b) the end date specified in the applicable Order. Trial Services are provided for evaluation purposes and not for production use. Customer shall have sole responsibility and Acquia assumes no liability for any Customer Data that Customer may choose to upload on the Trial Services. Trial Services may contain bugs or errors, and may be subject to additional terms. TRIAL SERVICES ARE NOT CONSIDERED "SERVICES" HEREUNDER AND ARE PROVIDED "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTY AND ACQUIA SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO THE TRIAL SERVICES. Acquia may, in its sole discretion, discontinue Trial Services at any time. For the avoidance of doubt, Trial Services may require acceptance of additional terms and conditions prior to Customer's permitted use.

2.3 Ancillary Programs. As part of the Subscription Services, Acquia may provide Customer with access to download certain Ancillary Programs for use with the Subscription Services. Acquia grants Customer during the Subscription Term a non-exclusive, non-transferable non-assignable, limited licensed to use such Ancillary Programs in object code (machine readable) format only on each site hosted by Acquia under an Order for Subscription Service to facilitate Customer access to, operation of, and/or use of the Subscription Services subject to the terms of this Agreement. Ancillary Programs shall only be used to upload, download and synchronize files between Customer's computer or other Customer owned or controlled devices and the Subscription Services.

3. SECURITY AND DATA PRIVACY

3.1. Security and Internal Controls. In accordance with Acquia's Security Annex incorporated herein by reference, Acquia shall (i) maintain a security framework of policies, procedures, and controls that includes administrative, physical, and technical safeguards for protection of the security and integrity of the Subscription Services, and of the Customer Data contained within the Subscription Services, using the capabilities of currently available technologies and in accordance with prevailing industry practices and standards, (ii) access and use the Customer Data solely to perform its obligations in accordance with the terms of this Agreement, and (iii) perform periodic testing by independent third party audit organizations, which include with Service Organization Controls 1 (SOC 1), SOC 2 audits and ISO 27001 certification or surveillance audits performed annually. In no event during the Subscription Term shall Acquia materially diminish the protections provided by the controls set forth in Acquia's then-current Security Annex.

3.2. Data Privacy. The terms of the Acquia Data Processing Addendum ("DPA") are hereby attached hereto and incorporated by reference and shall apply to the extent Customer Data includes Personal Data, as defined in the DPA.

EU, UK, Switzerland. To the extent Customer's use of the Subscription Services includes the processing of Customer Data by Acquia that are subject to the General Data Protection Regulation (EU) 2016/679 or the UK GDPR, as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (jointly "GDPR"), such data processing by Acquia as data processor complies with the requirements of the aforementioned regulations and any Personal Data transfer out of the European Union, the European Economic Area, the United Kingdom, and Switzerland shall be governed by the Standard Contractual Clauses as attached to the DPA, unless the Customer has opted out of those clauses. For the purposes of the **Standard Contractual Clauses**, Customer and its applicable Affiliates are each the data exporter, and Customer's acceptance of this Agreement, and an applicable Affiliate's execution of an Order Form, shall be treated as its execution of the Standard Contractual Clauses and Appendices to the extent that such clauses do not impose obligations on Ordering Activity that are inconsistent with the Federal law of the United States.

CCPA, CPRA. Where Customer's use of the Subscription Services includes the processing of California Consumer's Personal Information by Acquia that are subject to the California Consumer Protection Act of 2018 a, and its implementing regulations, as amended or superseded from time to time ("**CCPA**") including as amended by the California Privacy Rights Act of 2020 ("**CPRA**"), such data processing by Acquia as a "service provider" complies with the requirements of the CCPA.

Processing and Data Subject Requests. Acquia shall process personal data and personal information on behalf of and in accordance with Customer's instructions consistent with this Agreement and as necessary to provide the Subscription Services and will reasonably cooperate with Customer in its efforts to respond to requests by data subjects and/or California Consumers to exercise their rights under the GDPR or CCPA and to otherwise comply with the GDPR or CCPA.

3.3. Data Center Region. Customer may select the Data Center Region from those available for the applicable Subscription Services. Acquia will not move the selected Data Center Region and the Customer Data contained within such Data Center Region, without Customer's written consent or unless required to comply with the law or requests of a governmental or regulatory body (including subpoenas or court orders). Customer consents to Acquia's storage of Customer Data in, and transfer of Customer Data into, the Data Center Region Customer selects.

3.4. Compliance with Law. Acquia will comply with all laws applicable to the provision of the Subscription Services, including applicable security breach notification laws, but not including any laws applicable to the Customer's industry that are not generally applicable to information technology services providers.

4. CUSTOMER OBLIGATIONS AND PERMITTED USE OF AI FEATURES

4.1. Responsibilities. Customer shall (i) access and use the Services in accordance with this Agreement, applicable laws and government regulations and Acquia's Acceptable Use Policy attached hereto and incorporated herein by reference, (ii) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Acquia promptly of any such unauthorized access or use, and (iii) take commercially reasonable steps necessary to ensure the security and compliance of the Customer Applications.

4.2. Customer Data. Customer has and shall maintain all rights as are required to allow Acquia to provide the Subscription Services to Customer as set forth in this Agreement, including without limitation to send the Customer Data to Acquia pursuant to this Agreement and to allow Acquia to access, use, and store Customer Data to provide the Subscription Services pursuant to this Agreement. Customer is responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any Customer Data processed, stored, or transmitted through the Subscription Services for which regulations other than those set forth in the Security Annex apply. If, in the course of providing Subscription Services, Acquia agrees in writing to process such Customer Data and Customer has subscribed to any applicable Subscription Services, Acquia shall process it only as permitted under this Agreement and in

compliance with data protection legislation to which Acquia is subject as a service provider.

4.3 Restrictions. Customer shall not (i) license, sublicense, sell, resell, rent, lease, transfer, distribute or otherwise similarly exploit the Subscription Services or Ancillary Programs), (ii) use or permit others to use any security testing tools in order to probe, scan or attempt to penetrate or ascertain the security of the Subscription Services, (iii) copy, create a derivative work of reverse engineer, reverse assemble, disassemble, or decompile the Subscription Services, Ancillary Programs, or any part thereof or otherwise attempt to discover any source code or modify the Subscription Services or the Ancillary Programs), (iv) create a competitive offering based on the Subscription Services, and (v) disclose any benchmark or performance tests of the Subscription Services.

4.4 AI-Generated Content, AI Input, AI Output.

AI Input and AI Output are Customer Data.

Customer is solely responsible for the AI Input. Any AI Input that violates Acquia's AI Specific Terms and AI User Guidelines and Policy, infringes third-party rights, contains personal information which was obtained and/or is used in violation of any applicable data privacy law, any other applicable law, the AI User Information and Policy, or this Agreement is prohibited and shall not be used with Services.

Acquia may block AI Input, disable AI Output or the AI Features or the related Service(s), if Acquia in its sole discretion believes such violation has occurred or is imminent.

Acquia may use technologies, including those of third parties, to screen for and block AI Input and AI Output for such violations.

Customer may not use the AI Output to directly or indirectly train, test, or otherwise improve any AI or machine learning systems.

5. PROFESSIONAL SERVICES

5.1. Standard Professional Services. A description of Acquia's standard Professional Services offerings, including training, and workshops, may be found in the Documentation. Standard Professional Services may be identified in an Order without the need for issuance of an SOW.

5.2. Other Professional Services. For any non-standard Professional Services, Acquia will provide Customer with Professional Services as set forth in the applicable SOW. Each SOW will include, at a minimum (i) a description of the Professional Services and any Deliverable to be delivered to Customer; (ii) the scope of Professional Services; (iii) the schedule for the provision of such Professional Services; and (iv) the applicable fees and payment terms for such Professional Services, if not specified elsewhere.

5.3. Change Orders. Changes to an SOW or Order Form will require, and shall become effective only when, fully documented in a written change order (each a "**Change Order**") signed by duly authorized representatives of the parties prior to implementation of the changes. Such changes may include, for example, changes to the scope of work and any corresponding changes to the estimated fees and schedule. Change Orders shall be deemed part of, and subject to, this Agreement.

5.4. Designated Contact and Cooperation. Each party will designate in each SOW an individual who will be the primary point of contact between the parties for all matters relating to the Professional Services to be performed thereunder. Customer will cooperate with Acquia, will provide Acquia with accurate and complete information, will provide Acquia with such assistance and access as Acquia may reasonably request, and will fulfill its responsibilities as set forth in this Agreement and the applicable SOW. If applicable, while on Customer premises for Professional Services, Acquia personnel shall comply with reasonable Customer rules and regulations regarding safety, conduct, and security made known to Acquia.

6. FEES AND PAYMENT

6.1. Fees.

Customer shall pay all fees specified in each Order or SOW. Fees are payable in the currency set forth in the Order or SOW.. All amounts payable under this Agreement will be made without setoff or counterclaim, and without any deduction or withholding.

Subscription Services. Customer shall pay any applicable additional fees if Customer exceeds the allotted capacity or other applicable limits specified in the Order.

Fees are based on Subscription Services purchased, regardless of usage. All Subscription Services shall be deemed accepted upon delivery. The Subscription Services purchased cannot be decreased during the relevant Subscription Term.

Professional Services. All Professional Services shall be accepted in accordance with the acceptance criteria set forth in the relevant SOW. Customer shall reimburse Acquia for approved out-of-pocket expenses incurred by Acquia in connection with its performance of Services in accordance with Federal Travel Regulation (FTR)/Joint Travel Regulations (JTR), as applicable. Customer shall only be liable for such travel expenses as approved by Customer and funded under the applicable ordering document . Acquia will provide Customer with reasonably detailed invoices for such expenses.

6.2. Invoicing and Payment.

Subscription Services. Unless otherwise specified in an Order, fees for Subscription Services specified in an Order will be invoiced annuallyupon executing of the written order, fees for overages will be calculated and invoiced monthly in arrears.

Professional Services. Unless otherwise set forth in an SOW, all fees and expenses for standard Professional Services as described in Section 5.1 shall be invoiced 50% upon commencement and 50% upon completion, and all fees and expenses for non-standard Professional Services as described in 5.2 will be invoiced monthly in arrears on a time and materials basis.

Except as otherwise stated in the applicable Order or SOW, Customer agrees to pay all invoiced amounts within thirty (30) days of invoice receipt date. If Customer fails to pay any amounts due under this Agreement by the due date, in addition to any other rights or remedies it may have under this Agreement or by matter of law (i)reserved, and (ii) Acquia will have the right to charge interest at an interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

6.3. Taxes. Vendor shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with FAR 552.212-4(k).

7. PROPRIETARY RIGHTS

7.1. Subscription Services. Except for the rights expressly granted under this Agreement, Acquia and its licensors retain all right, title and interest in and to the Subscription Services and Documentation, including all related

intellectual property rights therein. Acquia reserves all rights in and to the Subscription Services and Documentation not expressly granted to Customer under this Agreement. Customer will not delete or in any manner alter the copyright, trademark, and other proprietary notices of Acquia.

7.2 Ancillary Programs, Third Party Tools. The Subscription Services (including Ancillary Programs) may interoperate with certain software products, including open-source software, owned by third parties and licensed directly to the Customer by such third party ("**Third Party Tool**"). Such Third Party Tool(s) is provided to the Customer without liability or obligation by Acquia and is subject to the applicable provider's terms and conditions and any such terms and conditions associated with such use are solely between Customer and such third party provider. Acquia does not provide any Support Services for Third Party Tools.

7.3. Customer Data and Customer Applications. As between Customer and Acquia, Customer is and will remain the sole and exclusive owner of all right, title and interest to all Customer Data and Customer Applications, including any intellectual property rights therein. Customer's use of any output from Third Party Tools shall be subject to and governed by the terms of use applicable to such Third Party Tool. Customer hereby grants Acquia, its Affiliates and applicable Authorized Contractors all necessary rights to host, use, process, store, display and transmit Customer Data and Customer Applications solely as necessary for Acquia to provide the Services in accordance with this Agreement. By using Ancillary Programs Customer grants Acquia permission to access Customer's computer or other devices to the extent necessary in enabling Ancillary Programs. Customer represents that it has, and warrants that it shall maintain, all rights as required to allow Acquia to compile, use, store, and retain aggregated Customer Data, including without limitation in combination with other Acquia customers' data, for internal or marketing uses (provided that no such marketing use shall include any information that can identify Customer or its customers). Subject to the limited licenses granted herein, Acquia acquires no right, title or interest from Customer or Customer licensors hereunder in or to Customer Data and Customer Applications, including any intellectual property rights therein. Customer reserves all rights in and to the Customer Data that are not expressly granted to Acquia pursuant to this Agreement.

7.4. Deliverables. Excluding any property that constitutes Outside Property, any Deliverables shall be the sole property of Customer upon Customer's payment in full of all associated Professional Services fees. Acquia shall execute and, at Customer's written request, require its personnel to execute any document that may be necessary or desirable to establish or perfect Customer's rights to the ownership of such Deliverables. For purposes of this Agreement, "**Outside Property**" means any and all technology and information, methodologies, data, designs, ideas, concepts, know-how, techniques, user-interfaces, templates, documentation, software, hardware, modules, development tools and other tangible or intangible technical material or information that Acquia possesses or owns prior to the commencement of Professional Services or which it develops independent of any activities governed by this Agreement, and any derivatives, modifications or enhancements made to any such property. Outside Property shall also include any enhancements, modifications or derivatives made by Acquia to the Outside Property while performing Professional Services hereunder, and any software, modules, routines or algorithms which are developed by Acquia during the term in providing the Professional Services to Customer, provided such software, modules, routines or algorithms have general application to work performed by Acquia for its other customers and do not include any content that is specific to Customer or which, directly or indirectly, incorporate or disclose Customer's Confidential Information.

7.5. Outside Property License. To the extent that Acquia incorporates any Outside Property into any Deliverables, then Acquia hereby grants Customer a limited, royalty-free, non-exclusive, non-transferable (subject to Section 14.11), without right to sublicense, license to use such Outside Property delivered to Customer solely as necessary for and in conjunction with Customer's use of the Deliverables.

8. CONFIDENTIALITY

8.1. Definition of Confidential Information. "**Confidential Information**" means all confidential or proprietary information of a party ("**Disclosing Party**") disclosed to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or reasonably should be understood to be confidential given the nature of information and the circumstances of disclosure. Without limiting the coverage of these confidentiality obligations, the parties acknowledge and agree that Confidential Information of each party shall include related benchmark or similar test results, other technology and technical information, security information, security audit reports, and business and marketing plans, except that Acquia may reference and use Customer's name, logos and the nature of the Services provided hereunder in Acquia's business development and marketing efforts.

8.2. Exceptions. Confidential Information shall not include information that (i) is or becomes publicly available without a breach of any obligation owed to the Disclosing Party, (ii) is already known to the Receiving Party at the time of its disclosure by the Disclosing Party, without a breach of any obligation owed to the Disclosing Party, (iii) following its disclosure to the Receiving Party, is received by the Receiving Party from a third party without breach of any obligation owed to Disclosing Party, or (iv) is independently developed by Receiving Party without reference to or use of the Disclosing Party's Confidential Information.

8.3. Protection of Confidential Information. The Receiving Party shall use the same degree of care used to protect the confidentiality of its own Confidential Information of like kind (but in no event less than reasonable care), and, except with Disclosing Party's written consent, shall (i) not use any Confidential Information of Disclosing Party for any purpose outside the scope of this Agreement and (ii) limit access to Confidential Information of Disclosing Party to those of its and its Authorized Contractors, Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have a duty or obligation of confidentiality no less stringent than that set forth herein.

8.4. Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent required by applicable law, regulation or legal process, provided that the Receiving Party (i) provides prompt written notice to the extent legally permitted, (ii) provides reasonable assistance, at Disclosing Party's cost, in the event the Disclosing Party wishes to oppose the disclosure, and (iii) limits disclosure to that required by law, regulation or legal process. Acquia recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

9. REPRESENTATIONS, WARRANTIES AND DISCLAIMERS

9.1. Acquia Representations & Warranties. Acquia represents and warrants that (i) Acquia has the legal authority to enter into this Agreement, (ii) the Subscription Services will materially conform with the relevant Documentation, (iii) the functionality and security of the Subscription Services will not be materially decreased during a Subscription Term, and (iv) Professional Services will be performed in a competent and workmanlike manner consistent with generally accepted industry standards.

9.2. Remedies. For any failure of any Subscription Services or Professional Services, as applicable, to conform to their respective warranties, Acquia's liability and Customer's sole and exclusive remedy shall be for Acquia, in the case of a breach of the warranty set forth in Section 9.1 (ii), (iii), and/or (iv), to use commercially reasonable efforts to correct such failure; or, in the case of a breach of the warranty set forth in Section 9.1 (iv) to re-perform the affected Professional Services. If the foregoing remedies are not commercially practicable, Acquia may, in its sole discretion, terminate the applicable Order or SOW upon providing Customer with written notice

thereof, and, as Customer's sole and exclusive remedy, refund to Customer (a) in the case of breach of the warranty set forth in Section 9.1(ii) or (iii), any Subscription Services fees paid by Customer with respect to the unexpired portion of the current Subscription Term for the non-conforming Subscription Services; or (b) in the case of breach of the warranty set forth in Section 9.1(iv), any fees paid by Customer for the portion of Professional Services giving rise to the breach.

9.3. Customer Representations & Warranties. Customer represents and warrants that (i) it has the legal authority to enter into this Agreement, and (ii) it will use the Services in accordance with the terms and conditions set forth in this Agreement and in compliance with all applicable laws, rules and regulations.

9.4. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN, ACQUIA MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, ORAL OR WRITTEN, STATUTORY OR OTHERWISE, AND ACQUIA HEREBY DISCLAIMS ALL IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY WITH RESPECT TO THE QUALITY, PERFORMANCE, ACCURACY OR FUNCTIONALITY OF THE SERVICES OR THAT THE SERVICES ARE OR WILL BE ERROR FREE OR WILL ACCOMPLISH ANY PARTICULAR RESULT, OR THAT THE AI OUTPUT DOES NOT VIOLATE THIRD-PARTY RIGHTS OR APPLICABLE LAW.

10. INDEMNIFICATION

10.1. Indemnification by Acquia. Acquia shall indemnify, have the right to intervene to defend and hold Customer harmless from and against any judgments, settlements, costs and fees reasonably incurred (including reasonable attorney's fees) resulting from any claim, demand, suit, or proceeding made or brought against Customer by a third party alleging that the use of the Subscription Services hereunder infringes or misappropriates the valid intellectual property rights of a third party (a "**Claim Against Customer**"); provided that Customer
(a) promptly gives Acquia written notice of the Claim Against Customer;
(b) gives Acquia control of the defense and settlement of the Claim Against Customer (provided that Acquia may not settle any Claim Against Customer unless the settlement unconditionally releases Customer of all liability); and
(c) provides to Acquia all reasonable assistance, at Acquia's expense. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. In the event of a Claim Against Customer, or if Acquia reasonably believes the Subscription Services may infringe or misappropriate, Acquia may in Acquia's sole discretion and at no cost to Customer (i) modify the Subscription Services so that they no longer infringe or misappropriate, without breaching Acquia's warranties hereunder, (ii) obtain a license for Customer's continued use of Subscription Services in accordance with this Agreement, or (iii) terminate Customer's subscriptions for such Subscription Services and refund to Customer any prepaid fees covering the remainder of the term of such subscriptions after the effective date of termination. Notwithstanding the foregoing, Acquia shall have no obligation to indemnify, defend, or hold Customer harmless from any Claim Against Customer to the extent it arises from (i) Customer Data or Customer Applications, (ii) use by Customer after notice by Acquia to discontinue use of all or a portion of the Subscription Services, (iii) use of Services by Customer in combination with equipment or software not supplied by Acquia where the Service itself would not be infringing, (iv) or Customer's breach of this Agreement.

10.2. Reserved.

10.3. Exclusive Remedy. This Section 10 states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim described in this Section.

11. LIMITATION OF LIABILITY

11.1. Limitation of Liability. EXCEPT FOR (I) EACH PARTY'S OBLIGATIONS SET FORTH IN SECTION 10 (MUTUAL INDEMNIFICATION), (II) INFRINGEMENT OR MISAPPROPRIATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, INCLUDING TRADE SECRETS, (III) DAMAGES FOR BODILY INJURY, DEATH, DAMAGE TO REAL OR TANGIBLE PERSONAL PROPERTY; OR (IV) ANY OTHER LIABILITY THAT MAY NOT BE LIMITED UNDER APPLICABLE LAW (THE "EXCLUDED MATTERS"), IN NO EVENT SHALL EITHER PARTY'S TOTAL AGGREGATE LIABILITY RELATING TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) EXCEED THE AMOUNT PAID OR PAYABLE BY CUSTOMER FOR THOSE SERVICES GIVING RISE TO SUCH CLAIM UNDER THE APPLICABLE ORDER FORM AND/OR SOW IN THE 12 MONTHS PRECEDING THE APPLICABLE INCIDENT.

11.2. Exclusion of Consequential and Related Damages. EXCEPT FOR THE EXCLUDED MATTERS, IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. . THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

12. TERM AND TERMINATION

12.1. Term of Agreement. This Agreement commences on the Effective Date and continues until otherwise terminated, by written agreement of the parties, in accordance with Section 12.3 or upon the expiration of the last Subscription Term or renewal thereof.

12.2. Renewal of Subscription Services. Except as otherwise specified in the applicable Order, the Subscription Services may berenewed for successive one-year period sby executing a written order..

12.3. Termination. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Acquia shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

12.4. Data Portability and Deletion. Upon request made by Customer within 7 days of termination or expiration of the Subscription Services, Acquia will make Customer Data and Customer Applications available to Customer for export or download as provided in the Documentation. At the end of such 7-day period, Acquia will delete or otherwise render inaccessible any Customer Data and Customer Applications, unless legally prohibited. Acquia has no obligation to retain the Customer Data for Customer purposes after this 7-day post termination period.

12.5. Survival. Section 7 (Proprietary Rights), 8 (Confidentiality), 9.4 (Disclaimer), 10 (Mutual Indemnification), 11 (Limitation of Liability), 12.4 (Data Portability and Deletion), 13 (Notices, Governing Law and Jurisdiction) and 14 (General Provisions) and any other rights and obligations of the parties hereunder that by their nature are reasonably intended to survive termination or expiration, shall survive any termination or expiration of this Agreement.

13. NOTICES, GOVERNING LAW AND JURISDICTION

13.1. Manner of Giving Notice. Except as otherwise specified in this Agreement, all legal notices of default, breach or termination ("**Legal Notices**") hereunder shall be in writing and shall be deemed to have been given upon (i) personal delivery, (ii) the fifth business day after being sent by certified mail return receipt requested, or (iii) the first business day after sending by a generally recognized international guaranteed overnight delivery service. Each party shall send all Legal Notices to the other party at the address set forth in the applicable Order Form or SOW, as such party may update such information from time to time, with, in the case of notices sent by Customer, a copy sent to the Acquia Legal Department at the address first set forth above. Billing-related notices to Customer will be addressed to the relevant billing contact designated by Customer on the applicable Order.

13.2. Governing Law and Jurisdiction. This Agreement shall be governed and construed in accordance with the Federal laws of theUnited States, excluding its conflicts of law rules. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act do not apply to the Agreement.

13.3. Waiver of Jury Trial. Each party hereby waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

14. GENERAL PROVISIONS

14.1. Import and Export Compliance. Each party shall comply with all applicable import, re-import, export and re-export control laws, treaties, agreements, and regulations. Export controls may include, but are not limited to, those of the Export Administration Regulations of the U.S. Department of Commerce (EAR), the Department of State International Traffic in Arms Regulations (ITAR), and country-specific economic sanctions programs implemented by the Office of Foreign Assets Control (OFAC), which may restrict or require licenses for the export of Items from the United States and their re-export from other countries. Each party represents that it is not named on any U.S. government denied-party list. Customer shall not permit users to access or use Services in a U.S.-embargoed country or in violation of any U.S. export law or regulation.

14.2. Anti-Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of the other party's employees or agents in connection with this Agreement. If a party learns of any violation of the above restriction, such party will use reasonable efforts to promptly notify the other party.

14.3. Federal Government End Use Provisions *(only applicable for the U.S.)*. If the Services are being or have been acquired with U.S. Federal Government funds, or Customer is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure or transfer of the Services, or any related documentation of any kind, including technical data, manuals or Acquia Property is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995), as applicable. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire the software and Services with only those rights set forth in this Agreement and any amendment hereto.

14.4. Subscription Service Analyses. Acquia may (i) compile statistical and other information related to the performance, operation and use of the Subscription Services, and (ii) use, and share data from the Subscription Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as 'Subscription Service Analyses"). Subscription Service Analyses will not incorporate any information, including Customer Data, in a form that could serve to identify Customer or an individual. Acquia retains all intellectual property rights in Subscription Service Analyses.

14.5. Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

14.6. Non-Solicitation. Customer agrees that during the term of each Order Form and/or SOW and for twelve (12) months thereafter, it will not recruit or otherwise solicit for employment any person employed by Acquia who participated in the performance of Services under the applicable Order Form and/or SOW. Nothing in this clause shall be construed to prohibit individual Acquia employees from responding to public employment advertisements, postings or job fairs of Customer, provided such response is not prompted by Customer intentionally circumventing the restrictions of this Section.

14.7. No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.

14.8. Public Relations. Customer agrees that Acquia may identify Customer as an Acquia customer in advertising, media relations, trade shows, the website, and other similar promotional activities, using Customer's name in accordance with Customer's trademark guidelines including, but not limited to, General Services Acquisition Regulation (GSAR) 552.203-71. Customer shall also assist Acquia in preparing a press release announcing Customer as a new Acquia Customer, with the view to publishing within 60 days following the Effective Date and in preparing a case study for external use that details Customer's use of the Services within 6 months following the Effective Date. Acquia shall not publish such press release or case study without Customer's prior, written approval as to its contents.

14.9. Waiver. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right.

14.10. Force Majeure. Excusable delays shall be governed by FAR 552.212-4(f) .

14.11. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

14.12. Assignment. Neither party may assign its rights and obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other party. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors, and permitted assigns.

14.13. Entire Agreement. This Agreement constitutes the entire agreement between the parties as it relates to the subject matter and supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning or relating to the same. Except as otherwise provided herein, no modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by both parties. To the extent of any conflict or inconsistency between the provisions of this Agreement, the Documentation, any Order Form or SOW, the terms of such Order Form or SOW shall prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in a PO, payment system, other order documentation or otherwise (excluding Order Forms and/or SOWs) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year last set forth below.

ACQUIA

By: _____

Name: _____

Title: _____

Date: _____

CUSTOMER

By: _____

Name: _____

Title: _____

Date: _____

ACQUIA ACCEPTABLE USE POLICY

General

This Acceptable Use Policy (this "Policy") describes prohibited uses of all services offered by Acquia Inc. and its affiliates (the "Services") and the website located at http://www.acquia.com and all associated sites (the "Acquia Site"). The examples described in this Policy are not exhaustive. We may non-materially modify this Policy at any time by posting a revised version on the Acquia Site. By using the Services or accessing the Acquia Site, you agree to the latest non-materially modified version of this Policy. If you violate the Policy or authorize or help others to do so, we may suspend or terminate your use of the Services in accordance with the Contract Disputes Act.

You are solely responsible for any material that you or your end users maintain, transmit, download, view, post, distribute, or otherwise access or make available using the Services. By using the Services, you represent that you own the content that you make available through Acquia's Services and all proprietary or intellectual property rights therein, or have the express written authorization from the owner to copy, use and display such content.

Prohibited Use of Services

A. No Illegal, Harmful, or Offensive Use or Content

You may not use, encourage, promote, facilitate or instruct others to use, the Services or Acquia Site for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive.
Prohibited activities or content include but are not limited to:

- **Illegal, Harmful or Fraudulent Activities**. Any activities that are illegal, that violate the rights of others, or that may be harmful to others, our operations or reputation, including (i) disseminating, promoting or facilitating child pornography, (ii) offering or disseminating fraudulent goods, services, schemes, or promotions, (iii) make-money-fast schemes, ponzi and pyramid schemes, (iv) phishing, or pharming, or (v) threatening, inciting, promoting, or encouraging hate speech, harassment, discrimination, or violence based on race, ethnicity, nationality, religion, gender, sexual orientation, disability, or any other protected characteristic.
- **Infringing Content**. Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- **Offensive Content**. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography.
- **Harmful Content**. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, malware, Trojan horses, worms, time bombs, or cancelbots.

B. No Security Violations

You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include but are not limited to:

- **Unauthorized Access**. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- **Interception**. Monitoring of data or traffic on a System without permission.
- **Falsification of Origin**. Forging TCPIP packet headers, email headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

C. No Network Abuse

You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include but are not limited to:

- **Unauthorized Access**. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- **Interception**. Monitoring of data or traffic on a System without permission.
- **Falsification of Origin**. Forging TCPIP packet headers, email headers, or any part of a message describing its origin or route. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

D. No Spam

You will not distribute, publish, send, or facilitate the sending of unsolicited mass email or other messages, promotions, advertising, or solicitations, like “spam". You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. You will not collect replies to messages sent from another Internet service provider if those messages violate this Policy or the acceptable use policy of that provider. All recipients in a Acquia customer or user's contact list must have given provable consent, online or otherwise, to receive email communication and for the specific content being sent to them. You must abide by the following rules:

- Email lists that were obtained by any means without consent are not allowed
- All email and recipient lists must adhere to the CAN-SPAM laws, as well as to any local spam laws for your location or the location of your recipient lists
- Email must abide by the rules outlined in this Policy
- No 3rd party unsubscribe methods are allowed

Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services or Acquia Site. We may:

- investigate violations of this Policy or misuse of the Services or Acquia Site; or

- remove, disable access to, or modify any content or resource that violates this Policy or any other agreement we have with you for use of the Services or the Acquia Site.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

Feedback Loops and Abuse Reporting

Acquia is registered with Internet Service Provider ("ISP") feedback loops and monitors abuse reports. These feedback loops notify Acquia when your or your user's contact marks a message as "spam". You and your users are subject to warnings, suspension or termination if Acquia receives a report containing a high number of spam reported against your or your user's account.

Bounce Rates

An account's bounce rate is subject to be monitored by Acquia. An account's bounce rate should consistently remain under 8% as many ISPs will begin blocking IPs for higher bounce rates. Accounts with high bounce rates are subject to warnings, suspension or termination. To avoid such consequences, ensure your list of contacts are reviewed and maintained regularly.

Plugins and Integrations

You and your users utilizing Acquia's available integrations and plugins must adhere to Acquia's policies, as well as those of the 3rd party system being integrated. If you are found to be violating Acquia's or an integrated 3rd party system's policy, your account will be subject to suspension or deletion.

Acquia Code of Business Conduct & Ethics

Acquia is committed to its Code of Business Conduct and Ethics. To the extent it may apply to a customer's use of Acquia services, customer agrees to comply with Acquia's Code of Business Conduct and Ethics, as may be updated from time to time.

Reporting of Violations of this Policy

If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please contact our Legal Department: legal@acquia.com.

AI Terms

Effective as of 17 September 2024

These AI Specific Terms and AI User Guidelines and Policy attached hereto and located at http://acquia.com/legal/ai-user-guidelines ("Guidelines") govern Customer use of generative AI features with the Acquia Services and are incorporated by reference into that certain subscription and services agreement between Customer and Acquia ("General Terms") (these AI Specific Terms, the Guidelines, and the General Terms are collectively referred to as "Terms").

Capitalized terms not defined here have the same meaning as defined in the General Terms.

1. Generating Content.

When using generative AI features, users may input or upload content, such as an audio file, video file, document, image, text, or other digital assets (including any output parameters, such as aspect ratio, style, etc.) to the Services (collectively, "Input"). Input may be used by the Services to generate an output, such as an image, text, text effects, vector graphic file, audio file, code, design templates, websites, or video file, which will be provided within the Services ("Output"). The Input and Output are Customer Data and all provisions governing Customer Data in the Terms apply to such Input and Output. The generative AI features, Input, and Output must be used in accordance with the Terms, which may be modified from time to time. Acquia reserves the right to disable, suspend, or terminate your right to use or access the generative AI features at any time in our sole discretion without prior notice.

2. Input.

Customer is solely responsible for Input. Customer shall not submit any Input that: (a) includes trademarks or other materials protected by third-party intellectual property rights, unless Customer has sufficient rights in such materials; (b) is intended to generate Output that is substantially similar to a third party's copyrighted work or is otherwise protected by third-party intellectual property rights, unless Customer has sufficient rights in such work; (c) contains personal information unless Customer complies with all data protection and privacy laws and regulations applicable to the personal information, including providing privacy notices and obtaining consent, where required; (d) violates applicable law; or (e) violates the Terms. Acquia may automatically block Input, in our sole discretion, which violates the rights of a third party, applicable law, or the Terms.

3. Output.

3.1. Customer Responsibilities. Customer is solely responsible for the creation and use of the Output and for ensuring the Output complies with the Terms; however, Acquia may use available technologies, vendors, or processes to screen for and block Output that may violate applicable law, the rights of a third party, or the Terms, before the Output may be delivered.

3.2 DISCLAIMER. Acquia disclaims all warranties, express or implied, regarding the Output, including any implied warranties that the Output will not violate the rights of a third party or any applicable law. For the avoidance of doubt, Output is Customer Data, and any indemnification obligations set forth in the General Terms shall not apply to Output.

3.3. Suitability of Output. Use of generative AI features may produce Output that is unexpected or unsuitable for some users. The Output may not be unique and other users of generative AI features may generate the same or similar Output. The Output may not be protectable by intellectual property rights.

3.4. No AI/ML Training. Customer shall not, and must not allow third parties to, use any content, data, output or other information received or derived from any generative AI features, including any Outputs, to directly or indirectly create, train, test, or otherwise improve any machine learning algorithms or artificial intelligence systems, including any architectures, models, or weights. Acquia shall not use any Customer Data to train AI/ML without the express written consent of Customer.

ACQUIA DATA PROCESSING ADDENDUM[1]

(including EU SCCs, UK IDTA, and US State Privacy Laws requirements)

This Data Processing Addendum (the "**DPA**") covers the Services (as further described below) provided by Acquia in, 53 State Street, 10th Floor, Boston, MA 02109, USA ("**Acquia**"), and any Acquia Affiliates, as applicable, that may Process Personal Data and which were sold either by Acquia directly or an authorized reseller ("**Reseller**") to the Customer specified on page of this DPA ("**Customer**") under a respective end user services agreement or similar contract ("**Agreement**"). This DPA is entered into by Acquia and the Customer effective as of the last signature date below.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Customer Affiliates, if and to the extent Acquia processes Personal Data for which such Customer Affiliates qualify as the Controller. In providing the Services to Customer, Acquia may Process Personal Data on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Personal Data. The Customer that is the contracting party to this DPA shall remain responsible for coordinating all communication with Acquia under this DPA and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Customer Affiliate(s).

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

DEFINITIONS.
In this DPA, the following terms shall have the meanings set out below:

"**Acquia**" means Acquia Inc., a company incorporated in Delaware and its primary address as 53 State Street, Boston, MA 02109, USA.

"**Acquia Affiliates**" means all Acquia Affiliates listed at https://www.acquia.com/about-us/legal/subprocessors.

"**Acquia Group**" means Acquia and Acquia Affiliates engaged in the Processing of Personal Data.

"**Annex**" herein means an appendix to the EU SCCs; as opposed to "Exhibit" which means an appendix to the DPA.

"**Controller**" means 'controller' or 'data controller' as defined in the GDPR, US State Privacy Laws, or analogous in other applicable Data Protection Laws.

"**Customer Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Acquia, but has not signed its own Order with Acquia and is not a "Customer" as defined under the Agreement.

"**Customer Group**" means Customer and any of its Customer Affiliates.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including – where applicable – , but not limited to,

- the **GDPR** (as further defined herein and which includes the applicable regulations for the European Union, the United Kingdom, and Switzerland),
- the **US State Privacy Laws** (as further defined herein and which include, but are not limited to, the applicable laws of California, Colorado, Connecticut, Utah, and Virginia)
- the **South Africa** Protection of Personal Information Act ("**POPIA**"),
- the Privacy Act 1988 of **Australia** ("**AUSPA**"),
- the **Canadian** Personal Information Protection and Electronic Documents Act ("**PIPEDA**").

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**EEA**" means the European Economic Area.

"**Exhibit**" herein means an appendix to the DPA; as opposed to "Annex" which means an appendix to the EU SCCs.

"**GDPR**" means

- **[European Union]** the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (also the "**EU GDPR**"),
- **[United Kingdom]** the "**UK GDPR**" (as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019), and

---

1 **How to execute this DPA:**

- This DPA has been pre-signed by Acquia (end of DPA main body on **page**).
- Complete any information required in
  - The signature boxes at the end of the DPA main body on **page** ,
  - The information for the EU SCC Annexes I and II (**Exhibit 2** to this DPA)
  - The information for the UK IDTA **(Exhibit 3** to this DPA)
- Send the completed and signed DPA via email to privacy@acquia.com.
- Any additions, removals, or other modifications to the terms of this DPA (handwritten or otherwise) will render this DPA ineffective unless explicitly agreed to by Acquia separately in writing.

- **[Switzerland]** the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1;), and from 01 January 2023 onwards, the revised Swiss Federal Act on Data Protection of 25 September 2020 (both, as applicable, "**Swiss GDPR**").

"**Personal Data**" means all data which may be defined as 'personal data', 'personal information', 'personally identifiable information' or an analogous term as defined in the GDPR, US State Privacy Laws, or other applicable Data Protection Laws that is subjected to the Services under Customer's Agreement.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means 'processor' or 'data processor' as defined in the GDPR, US State Privacy Laws, or analogous in other applicable Data Protection Laws, including 'service provider" as that term is defined by the CCPA.

"**Product Notice**" means the respective notice describing privacy-related description of the Services, as available on Acquia's website at https://docs.acquia.com/guide/ (marked as '**GDPR Product Notice'** or **'Privacy Product Notice**').

"**Services**" means the services provided by Acquia to Customer as agreed in the Agreement.

"**Standard Contractual Clauses**" means

(i) where the **EU GDPR or Swiss Federal Act on Data Protection** apply, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"; completed Annexes to the EU SCCs attached hereto in **Exhibit 2)**; and

(ii) (ii) where the **UK GDPR** applies, the "Standard Data Protection Clauses issued by the Commissioner under S119A(1) Data Protection 2018 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force 21 March 2022" ("**UK IDTA**"), as attached hereto in **Exhibit 3**.

"**Sub-processor**" means any Processor engaged by Acquia or a member of the Acquia Group.

"**Supervisory Authority**" means an independent public authority, which is established by an EU Member State pursuant to the GDPR, US Stata Privacy Laws, or other applicable Data Protection Laws.

"**US State Privacy Laws**" [2] means the applicable privacy laws enacted by a state of the United States of America, including, but not limited to,

- [California]
  - the California Consumer Privacy Act of 2018 (California Civil Code §§1798.100 to 1798.199) and its implementing regulations, as amended or supplemented from time to time (the "**CCPA**");
  - the California Privacy Rights Act of 2020 (2020 Cal. Legis. Serv. Proposition 24 codified at California Civil Code §§ 1798.100 et seq.), and its implementing regulations, as amended or supplemented from time to time (the "**CPRA**");
- [Colorado] the Colorado Privacy Act, C.R.S.A. § 6-1-1301 et seq. (SB 21-190), including any implementing regulations and amendments thereto (the "**CPA**");
- [Connecticut] the Connecticut Data Privacy Act, S.B. 6 (Connecticut 2022), including any implementing regulations and amendments thereto (the "**CTDPA**");
- [Delaware] the Delaware Personal Data Privacy Act (House Bill 154 (2023)), including any implementing regulations and amendments thereto (the "**DPDPA**");
- [Florida] the Florida Digital Bill of Rights (Senate Bill 262 (2023)), including any implementing regulations and amendments thereto (the "**FDBR**")
- [Indiana] the Indiana Consumer Data Protection Act, Senate Bill 5 (2023), including any implementing regulations and amendments thereto (the "**Indiana CDPA**");
- [Iowa] the Iowa Consumer Data Protection Act, Senate File 262, including any implementing regulations and amendments thereto (the "**Iowa CDPA**");
- [Montana] the Montana Consumer Data Privacy Act, S.B. 384, including any implementing regulations and amendments thereto (the "**MCDPA**");
- [New Jersey] the New Jersey Senate Bill 332 for An Act concerning commercial Internet websites, , online services, consumers, and personally identifiable information, including any implementing regulations and amendments thereto (the "**NJPA**")
- [Oregon] the Oregon Consumer Privacy Act, Senate Bill 619, including any implementing regulations and amendments thereto (the "**OCPA**");
- [Tennessee] the Tennessee Information Protection Act, Public Chapter No. 408, including any implementing regulations and amendments thereto (the "**TIPA**");
- [Texas] the Texas Data Privacy and Security Act, including any implementing regulations and amendments thereto (the "**TDPSA**");
- [Utah] the Utah Consumer Privacy Act, Utah Code § 13-61-101 et seq. (SB 0227), including any implementing regulations and amendments thereto (the "**UCPA**");
- [Virginia] the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 et seq. (SB 1392), including any implementing regulations and amendments thereto (the "**VCDPA**").

1. DATA PROCESSING.

1.1 **Scope and Roles**. This DPA applies when Personal Data is Processed by Acquia as part of Acquia's provision of Services as agreed in the Agreement and the applicable Order. In this context, Customer (or a relevant Customer Affiliate) is the Controller (or, as the case may be, a Processor processing Personal Data on behalf of a third-party Controller) and Acquia is the Processor (or sub-Processor) with respect to

[2] Date of the respective US State Privacy Laws expected to come into effect: FDRB and OCPA: 01 July 2024; MCDPA: 01 Oct 2024; Iowa CDPA, TDPSA and DPDPA: 01 Jan 2025; NJPA: 16 January 2024; TIPA: 01 Jul 2025; Indiana CDPA: 01 Jan 2026.

Personal Data.

1.2 **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

1.3 **Acquia's Processing of Personal Data**. Acquia shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions as set forth in Section 2.

1.4 **Details of the Processing**. The subject matter of Processing of Personal Data by Acquia is the performance of the Services pursuant to the Agreement. Acquia will Process Personal Data as necessary to perform the Services pursuant to the Agreement and for the term of the Agreement. The type of personal data and categories of data subjects, the nature and purpose of the processing are further specified in the respective Product Notice incorporated herein.

1.5 **Compliance with Laws**. Each party will comply with all applicable laws, rules and regulations, including the Data Protection Laws.

2. CUSTOMER INSTRUCTIONS.

2.1 Acquia will process Personal Data in accordance with Customer's instructions. The parties agree that this DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Acquia in relation to the Processing of Personal Data. Additional or modified instructions require a documentation similar to this DPA and any such instructions leading to additional efforts by Acquia beyond the scope of the Services agreed in the Agreement and the Order may result in additional service fees payable by Customer that need to be documented in writing. Customer shall ensure that its instructions comply with Data Protection Laws and that the Processing of Personal Data in accordance with Customer's instructions will not cause Acquia to be in breach of Data Protection Laws or Standard Contractual Clauses.

2.2 Acquia shall notify the Customer if in Acquia's opinion any instruction Acquia receives pursuant to this Section 2 breaches (or causes either party to breach) any Data Protection Laws.

2.3 If Customer (or the relevant Customer Affiliate) is a Processor, Customer warrants to Acquia that Customer's instructions and actions, including electing Acquia as a (sub-)Processor, including any potential cross-border transfers, have been authorized by the relevant third-party Controller.

3. ACQUIA PERSONNEL.

3.1 **Limitation of Access**. Acquia shall ensure that Acquia's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

3.2 **Confidentiality**. Acquia shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training in their responsibilities, and have executed written confidentiality agreements. Acquia shall ensure that such confidentiality agreements survive the termination of the employment or engagement of its personnel.

3.3 **Reliability**. Acquia shall take commercially reasonable steps to ensure the reliability of any Acquia personnel engaged in the Processing of Personal Data.

3.4 **Data Protection Officer**. Acquia shall have appointed, or shall appoint, a data protection officer if Data Protection Laws require such appointment. Any such appointed person may be reached at privacy@acquia.com.

4. TECHNICAL AND ORGANIZATIONAL MEASURES, CERTIFICATIONS, AUDITS.

Acquia has implemented and will maintain the technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Customer Data as described in the Acquia Security Annex (available online at https://www.acquia.com/sites/default/files/legal/acquia-security-annex.pdf (the version applicable as of signature of this DPA is attached hereto as Exhibit 1)) also incorporated herein. Acquia regularly monitors compliance with these measures. Acquia has obtained third-party certifications and audits set forth in the Acquia Security Annex. In addition, the Acquia Security Annex specifies how Acquia allows for, and contributes to, audits.

If the EU SCCs or UK IDTA apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the EU SCCs. Nothing in this section of the DPA varies or modifies any Standard Contractual Clauses or Data Protection Laws or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Laws.

5. SUB-PROCESSORS.

5.1 **Sub-processors**. Customer acknowledges and agrees that (a) Acquia's Affiliates may be retained as Sub-processors; and (b) Acquia and its Affiliates respectively may engage third-party Sub-processors in the performance of the Services. Acquia or its Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Customer hereby consents to Acquia's use of Sub-processors as described in this Section.

5.2 **List of Current Sub-processors and Information about New Sub-processors**. Acquia shall make available to Customer a current list of Sub-processors for the Services at https://www.acquia.com/about-us/legal/subprocessors. Customer may subscribe to receive notifications of new sub-processors on the aforementioned website.

5.3 **Objection Right for new Sub-processors**. Customer may object to Acquia's use of a new Sub-processor by notifying Acquia promptly in writing within 10 business days after Acquia's update in accordance with the mechanism set out in Section 5.2 above. In the event Customer objects to a new Sub-processor: (i) Customer may immediately terminate the Agreement on giving written notice to Acquia; or

(ii) where that objection is not unreasonable, Acquia will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid processing of Personal Data by the objected-to new Sub processor without unreasonably burdening Customer. If Acquia is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, without prejudice to Section 5.3 (i), Customer may terminate the applicable Order(s) in respect only to those Services which cannot be provided by Acquia without the use of the objected-to new Sub-processor, on the condition that Customer provides such termination notice within 90 days of being informed of the engagement of the Sub-processor as described in Section 5.2 above. If Customer terminates the Agreement under this Section 5.3, Acquia will then refund Customer any prepaid fees covering the remainder of the term of such terminated Order(s) following the effective date of termination with respect of such terminated Services. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Sub-processor.

5.4 **Acquia's Liability for Sub-processors**. Acquia shall be liable for the acts and omissions of its Sub-processors to the same extent Acquia would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise agreed.

6. RIGHTS OF DATA SUBJECTS.

6.1 Acquia shall, to the extent legally permitted, promptly notify Customer if Acquia receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("**right to be forgotten**"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). Considering the nature of the Processing, Acquia shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Acquia shall upon Customer's request assist Customer in responding to such Data Subject Request, to the extent Acquia is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws.

6.2 To the extent legally permitted, Customer shall be responsible for any costs arising from Acquia's provision of such assistance as described in Section 6.1. Acquia shall bear the sole cost of the provision of such assistance if Acquia or its Sub-processors are required under Data Protection Laws to perform the activities or provide the information requested by the Customer.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION.

Acquia maintains a security incident management policy and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Acquia or its Sub-processors of which Acquia becomes aware (a "Personal Data Incident"), as required to assist the Customer in ensuring compliance with its obligations to notify the Supervisory Authority in the event of Personal Data breach. Acquia shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Acquia deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Acquia's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users.

8. DATA PROTECTION IMPACT ASSESSMENT AND ASSISTANCE.

Upon Customer's request, Acquia shall provide Customer with reasonable cooperation and assistance needed: (i) to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services; and (ii) in connection with the Customer's obligations under Articles 32 to 34 (inclusive) of the GDPR. Acquia shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section.

9. RETURN OR DELETION OF PERSONAL DATA.

Acquia shall (at the Customer's sole option) return Personal Data to Customer and/or delete Personal Data after the end of the provision of Services relating to Processing in accordance with the timeframe specified in the Agreement, unless applicable law requires storage of Personal Data.

10. TRANSFERS OF PERSONAL DATA, ADDITIONAL SAFEGUARDS, GOVERNMENT DATA PRODUCTION REQUEST.

10.1 **Geographic Region.** Customer may select the geographic region in which Personal Data is housed from those available for the applicable Services. Once Customer has made its choice, Acquia will not move the Personal Data without Customer's prior written consent or unless required to comply with applicable law.

10.2 **Standard Contractual Clauses.**

10.2.1 **Current Standard Contractual Clauses.**

10.2.1.1 **Personal Data from the EU, EEA, Switzerland:** Where Acquia processes Personal Data that originates from the European Union, the EEA, and/or Switzerland, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the EU SCCs as follows:

10.2.1.1.1 **Module Two** of the EU SCCs shall apply where Customer or a relevant Customer Affiliate is a Controller and **Module Three** shall apply where Customer or a relevant Customer Affiliate is a Processor;

10.2.1.1.2 Regarding **Clause 7** of the EU SCCs ("Docking Clause"), the optional docking clause shall apply;

10.2.1.1.3 Regarding **Clause 9** of the EU SCCs ("Use of sub-processors", Option 2 of Clause 9 (a) ("General Written Authorisation") shall apply with at least 30-day prior notice;

10.2.1.1.4 Regarding **Clause 11** of the EU SCCs ("Redress"), the optional language in Clause 11 (a) shall not apply;

10.2.1.1.5 Regarding **Clause 17** of the EU SCCs ("Governing Law"), Option 2 shall apply with the proviso that if the data exporter's EU Member State does not allow for third-party beneficiary rights, then the law of the Federal Republic of Germany shall apply;

10.2.1.1.6 Regarding **Clause 18 (b)** of the EU SCCs ("Choice of forum and jurisdiction"), the Parties agree that the choice of venue in the Agreement shall apply to this DPA as well unless the venue is not in an EU Member State, in which case the courts disputes under this DPA shall be resolved by the courts of Munich, Germany.

10.2.1.1.7 **Annex I** and **Annex II** of the EU SCCs shall be deemed completed with the information as set out in Exhibit 2 to this DPA.

10.2.1.2 **Personal Data from the UK:** Where Acquia processes Personal Data that originates from the United Kingdom, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the UK IDTA as attached hereto as **Exhibit 3**, unless the Customer has opted out of those clauses.

10.2.1.3 **Personal Data from Switzerland:** Where Acquia processes Personal Data that originates from Switzerland, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the EU SCCs, unless the Customer has opted out of those clauses with the proviso that the place of habitual residence in clause 18 (c) of the EU SCCs shall also include Switzerland.

10.2.2 **Follow-up Standard Contractual Clauses.** If Acquia transfers Personal Data to a Sub-processor located outside the EEA (including the United Kingdom if it has not been granted an adequacy decision by the European Commission) or otherwise makes a transfer (including onward transfer) of Personal Data, that, in the absence of either party and/or Sub-Processor (as applicable) being bound by the Standard Contractual Clauses or any successor clauses issued by a competent body from time to time, would cause either party and/or a Sub-processor to breach any Data Protection Laws, then Acquia shall ensure it has in place Standard Contractual Clauses with the relevant Sub-processors, and the Parties shall reasonably amend any data privacy agreement between the Parties (so that they apply at least for the term of the Agreement).

11. DATA PRODUCTION REQUEST AND ADDITIONAL SAFEGUARDS.

11.1 If Acquia receives a mandatory request, order, demand, notice or direction from any government agency or other third party ("**Requestor**") to disclose any Personal Data whether or not in writing and whether or not referencing any Data Protection Laws or identifying any specific Data Subjects ("**Data Production Request**"), in addition to Clause 5(d)(i) of the EU SCCs, Acquia shall deal with the Data Production Request in accordance with the following terms:

11.2 Acquia shall use every reasonable effort to redirect the Requestor to make the Data Production Request directly to the Customer.

11.3 Acquia shall not disclose any Personal Data to any person in response to a Data Production Request unless either it is under a compelling statutory obligation to make such disclosure, or (having regard to the circumstances and the rights and freedoms of any affected Data Subjects) there is an imminent risk of serious harm that merits disclosure in any event (for example, to protect individuals' vital interests).

11.4 Where, in accordance with this Section 10, disclosure of the Personal Data is required in response to a Data Production Request, Acquia shall notify the Customer in writing in advance (setting out all relevant details) and shall thereafter provide all reasonable cooperation and assistance to the Customer and, if requested by the Customer, assist it with any application, injunction, order or request to prevent (or where that is not possible, to delay) the disclosure of any Personal Data.

11.5 Except where Acquia is prohibited under the law applicable to the Requestor from prior notification, Acquia shall use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the Data Protection Laws.

11.6 To the extent permitted under the Data Production Request, Acquia shall notify and consult with the relevant Supervisory Authority in respect of the Data Production Request, and at all times thereafter cooperate with the Supervisory Authority and the Customer to deal with and address the Data Production Request. Acquia shall, if permitted under the law applicable to the Requestor, suspend (or where not possible, apply to suspend) the Data Production Request, so that it can notify and consult with the Customer and the relevant Supervisory Authority.

12. CCPA/CPRA PROVISIONS

12.1 **Applicability of the CCPA/CPRA.** To the extent Acquia Processes Personal Data governed by CCPA and/or CPRA on behalf of the Customer or a relevant Customer Affiliate, this Section 12 shall apply additionally; in case of discrepancies between this Section 12 and any other clause of this DPA, its Exhibits, or the Agreement, this Section 12 shall prevail.

12.2 **Definitions.** For this Section 12 of this DPA**,** the following terms shall have the meanings set out below:

"Business Purpose" has the meaning provided in § 1798.140(d) of the California Civil Code, as amended or supplemented from time to time.

"Consumer Rights Request" means a verified communication from a consumer requesting to access their rights under the CCPA.

"Personal Information" has the meaning provided in § 1798.140(o)(1) of the California Civil Code, as amended or supplemented from time to time.

12.3 **Relationship of Parties.** The Parties agree that in this context,

Customer or the relevant Customer Affiliate is the 'business', and

Acquia is solely the 'service provider' with respect to Personal Information,

as such terms are defined in the CCPA/CPRA.

12.4 **Business Purpose and Data Processing.** Customer/Customer Affiliate may disclose Personal Information to Acquia when necessary to perform a Business Purpose. Customer represents and warrants to Acquia that such disclosures of Personal Information shall be consistent with the requirements set forth in the CCPA/CPRA. Acquia shall Process Personal Information on behalf of the Customer/Customer Affiliate in accordance with and for the Business Purpose.

12.5 **Do Not Sell.** Acquia shall not sell Personal Information, nor shall it retain use, or disclose Personal Information, except as necessary to perform the Business Purpose, or as otherwise authorized by the CCPA/CPRA.

12.6 **Consumer Rights Requests**. Acquia shall notify Customer promptly if it receives a Consumer Rights Request concerning the processing of Personal Information and, in any event, in a reasonable amount of time for Customer to meet its obligations to respond to such Consumer Rights Request under the CCPA. Acquia shall not respond to any Consumer Rights Request concerning Personal Information unless expressly instructed to do so by Customer, or otherwise required by law. To the extent Customer, in its use of the Services, does not have the ability to address a Consumer Rights Request, Acquia shall upon Customer's request assist Customer in responding to such Consumer Rights Request, to the extent Acquia is legally permitted to do so and the response to such Consumer Rights Request is required under the CCPA. To the extent legally permitted, Customer shall be responsible for any costs arising from Acquia's provision of such assistance.

13. LIABILITY.
The total and aggregate liability of each party under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.

14. TERM AND TERMINATION OF THE DPA.
This DPA will become legally binding once Acquia has received a countersigned DPA from Customer, in accordance with the instructions set forth below, and the DPA shall continue in force until the termination of the Agreement.

The parties hereto have executed this DPA as of the day and year last set forth below.

CUSTOMER: (data exporter)	_____	**ACQUIA INC.** (data importer)	
Business Address:	_____	Business Address:	53 State Street, Boston, MA 02109, USA
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	Stephan Dobrowolski
Title:	_____	Title:	Associate General Counsel / Global Privacy Officer
E-mail:	_____	E-mail:	privacy@acquia.com
Date of signature:	_____	Date of signature:	_____

Exhibit 1
to the ACQUIA GDPR DATA PROCESSING ADDENDUM
Security Annex

Defined terms not otherwise defined herein shall have the means ascribed to them in the Agreement or DPA. In case of a conflict between this Security Annex and the Agreement or DPA, the Agreement or the DPA shall prevail.

1. Security Policy.

Acquia maintains a company-wide information security management system and control program that includes written security policies, standards and procedures based upon ISO/IEC 27001:2013 (collectively, the "**Acquia Information Security Policy**"). The Acquia Information Security Policy requires adherence to the following security principles (individually and collectively "Security Principle(s)"):

a. The identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of Customer Data to the extent that such Customer Data is provided to Acquia and maintained or processed by Acquia during its provision of Services by utilizing key operations and security practices such as:
   i. Secure software development practices;
   ii. Secure operating procedures and vulnerability management;
   iii. Ongoing employee training;
   iv. Controlling physical and electronic access to Customer Data, and
   v. Means for detecting and preventing intrusions and security system failures on critical systems.

b. That Acquia follow the Security Principle of least privilege access, allowing only active Acquia employees and contractors access to records containing Customer Data and limit such access to those persons who are reasonably required to know such information in order to accomplish a valid business purpose or to comply with record retention regulations;

c. That Customer Data that is identified as such to Acquia by the customer at intake, is secured appropriately commensurate to the nature of Customer Data, including any individual personal data provided to Acquia by Customer as set forth in this Annex, using commercially available and industry accepted controls and precautionary measures;

d. That commercially reasonable standards are followed with respect to strong change-control procedures and technical controls that enforce segregation of duties, minimum necessary dataset, and access controls;

e. Monitoring of operations and maintaining procedures to ensure that security protocols are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Customer Data, and continuously improving information safeguards as necessary to mitigate risks;

f. A security patch and vulnerability management process based on accepted industry standard practices and protocols, including, monitoring threats, and responding to vulnerabilities reported by third parties; and

g. A security incident response and disaster recovery planning, including documentation of responsive actions taken in connection with any security incident related to Customer Data.

2. Security Practices and Processes.

a. Customers are responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any Customer Data processed, stored, or transmitted through the Subscription Services for which regulations other than those set forth in this Annex apply. If, while providing Subscription Services, Acquia agrees in writing to process such Customer Data and Customer has subscribed to any applicable Subscription Services, Acquia shall process it only as permitted under this Agreement and in compliance with the DPA and applicable data protection legislation to which Acquia is subject as a service provider. If Acquia agrees to receive Customer Data from Customer, Acquia will manage and/or process such Customer Data pursuant to the security requirements, obligations, specifications and event reporting procedures as set forth in this Annex, the DPA, and the Agreement, and any amendments thereto.

b. Acquia will comply with secure software development practices consistent with industry accepted standards and practices.

c. Acquia restricts access to Customer Data and systems by users, applications, and other systems. These controls include (i) controls to systems and data, limited to properly authenticated and authorized individuals based on principles of least privilege and need-to-know; and (ii) physical access controls, as described below. Acquia will limit access to Customer Data to the minimum necessary dataset required in order to perform the relevant Service(s).

d. Acquia shall comply with the Acquia Physical Security Policy, as may be updated from time to time, and which shall include access and asset management controls (e.g., electronic locks, access badges, and video surveillance) that provide a physically secure environment.

e. Acquia logs access to controlled systems and records, including successful and failed system access attempts, and restricts the connection times of users. Acquia will use unique logins on all network equipment, whenever commercially reasonable.

f. Acquia maintains processes to identify and deploy security patches in a timely manner. Unless otherwise expressly agreed in writing, "timely" means that Acquia will introduce a fix or patch as soon as commercially reasonable after Acquia becomes aware of the security problem or availability of a fix or patch.

3. Patch and Vulnerability Management.

a. Acquia follows commercially reasonable best practices for centralized patch management, criticality ranking and patching time frame requirements for all Acquia-operated systems, switches, routers, appliances, servers, and workstation PC's, as applicable.

b. Where feasible, Acquia ensures that trusted, commercially available anti-virus software is installed, enabled, and kept current on Acquia servers and systems used in accessing, processing, transmitting, or storing Customer Data.

c. Acquia maintains trusted, current, commercially available anti-malware protection capabilities on Acquia devices, particularly those used for accessing, processing, transmitting, or storing Customer Data.

d. Acquia maintains a vulnerability management solution for devices connected to Acquia's LAN. Such solution is designed to regularly assess Acquia's network for known vulnerabilities.

4. Security Monitoring.

a. Acquia has a designated security team which monitors Acquia's control environment which is designed to prevent unauthorized access to or modification of Acquia's Customer Data. Acquia regularly monitors controls of critical systems, network, and procedures to validate proper implementation and effectiveness in addressing the threats, vulnerabilities and risks identified. This monitoring is variable by the criticality, exposure, and the system's assets and may include: (i) internal risk assessments; (ii) validation of Multi-Factor Authentication for select environments; (iii) third party compliance, including hosting services and third-party components; and (iv) assessing changes affecting systems processing authentications, authorizations, and auditing.

b. Acquia performs periodic vulnerability assessments on Acquia applications and systems. Penetration tests are performed either by Acquia or by an established, reputable independent third party.

5. Security of Data Processing.

Acquia has implemented and will maintain technical and organizational measures inclusive of administrative, technical, and physical safeguards to ensure a level of security appropriate to the risk of the data processing for the Acquia Services as described in this Annex (the "Security Measures"). These Security Measures may be changed by Acquia from time to time during the Term of the Agreement to take into account advancements in available security technologies. However, Acquia will not materially decrease the overall security of the Services during a Subscription Term.

The Security Measures may include, but will not be limited to, the following measures for ensuring the ongoing confidentiality, integrity, and availability of Customer Data to prevent unauthorized access, use, modification or disclosure of Customer Data:

a. Background Checks.

Performance of background checks on all personnel, as well as execution of non-disclosure commitments prior to employment and acknowledgment of professional behavior in the workplace documents, which includes anti-harassment and code of business conduct and ethics.

b. Training.

Security and privacy awareness training, inclusive of acknowledgment and agreement to abide by organizational security policies, for all personnel upon hire and annually thereafter.

c. Customer Data.

Pseudonymization or encryption of Customer Data in transit and at rest utilizing industry-standard mechanisms for certain Acquia Services.

A process for regularly testing, assessing and evaluating the effectiveness of administrative, technical and physical safeguards for ensuring the security of the processing, transmission or storage of Customer Data through external and internal audits as further described below.

Preventing access, use, modification, or disclosure of Customer Data except by authorized Acquia personnel (1) to provide the Subscription Services and prevent or address service or technical problems, (2) as compelled by law, or (3) as Customer expressly permits in writing; in any event pursuant to the terms set forth in an applicable DPA.

d. Availability.

The ability to restore the availability and access to Customer Data in a timely manner in the event of an incident impacting the availability of the Services by maintaining a backup solution for disaster recovery purposes.

e. Logging and Monitoring.

Logging and monitoring of security logs via a Security Incident Event Management ("**SIEM**") system and alerting to a dedicated Incident Response team upon the detection of suspicious system and/or user behaviors.

f. Vulnerability Triaging.

Processes and tooling for regularly identifying, assessing and triaging vulnerabilities based on industry-standard guidelines.

g. Policies

Maintenance of a comprehensive set of security and privacy policies, procedures and plans that are reviewed on at least an annual basis and provide guidance to the organization regarding security and privacy practices; and,

h. Sub-processors.

Processes for evaluating prospective and existing Sub-processors to ensure that they have the ability and commit to appropriate administrative, technical and physical measures to ensure the ongoing confidentiality, integrity and availability of Customer Data.

By implementing the Security Measures detailed above Acquia, considers the risks that are related to data processing, in particular the ones resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

6. Secure Data Transmissions.

Any Customer Data that Acquia transmits over a public communications network will be protected during transmission by using, or making available, industry accepted standards such as TLS, SSH and VPNs.

7. Data and Media Disposal.

Acquia maintains procedures that align with industry standards, such as NIST SP 800-88, regarding the disposal of both tangible property and electronic files containing Customer Data, considering available technology so that Customer Data cannot be reconstructed and read.

8. Backup and Retention.

Acquia will backup systems used to provide services to Customer to ensure adequate recovery capabilities in accordance with the schedule set forth in the Documentation for the applicable Services. Back-ups will be appropriately protected to ensure only authorized individuals are able to access the Customer Data, including but not limited to encryption of data stored off-site in electronic media and appropriate classification and protection of hard copy records, as applicable. If not separately backed up, Acquia will secure any files containing Customer Data against unauthorized access in accordance with the terms of the Agreement.

9. Customer Data.

Acquia will comply with those laws and regulations applicable to the provision of the Services concerning the confidentiality, security, and processing of any Customer Data that it receives from Customer. In the event Acquia processes types of Customer Data that are subject to additional regulatory requirements due to the nature of the data or its place of origin (as defined in section 2a above) Acquia will reasonably cooperate with Customer to arrange compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g. EU Standard Contractual Clauses, Business Associate Agreement governing Protected Health Information), implementation of additional security controls required by such law, completion of regulatory filings applicable to Acquia, and participation in relevant regulatory audits as applicable from Section 17 below ("Customer Audits.").

10. Security Incident Management and Remediation.

For purposes of this Annex, a "**Security Incident**" means (i) the loss of, (ii) unauthorized acquisition, use or disclosure of, or (iii) unauthorized access to, Customer Data resulting from a security breach of the Acquia platform. Acquia maintains a response function capable of identifying and assessing the seriousness and extent of a Security Incident, mitigating the effect of a Security Incident, conducting root cause analysis, implementing, and documenting remedial action plans, and preventing the recurrence of Security Incidents. Acquia has an established set of procedures to ensure personnel and contractors promptly report actual and/or suspected breaches of security. Acquia keeps an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents, as well as performing required recovery actions to remedy the impact.

a. Security Incidents on Acquia's platform are logged and reviewed, secured, and retained as required by applicable laws and regulations.

b. In the case of a Security Incident that relates to Customer Data, Acquia shall (a) promptly assess and contain such Security Incident, (b) notify Customer, without undue delay, upon becoming aware of such Incident, and in no case later than forty-eight (48) hours after Acquia has become aware of such Security Incident, via a Support ticket to each of the individuals identified by Customer for distribution of such Support Tickets (or such other addresses as may be provided by Customer from time to time) and provide regular status updates to Customer regarding the investigation at a frequency reasonably requested by Customer depending upon the severity of such Incident, (c) as applicable, provide reasonable cooperation and assistance to Customer needed to fulfill Customer's obligations related to Customer's use of the Services, as applicable, and (d) immediately take all steps reasonably necessary and within Acquia's reasonable control, including without limitation, those reasonably requested by Customer, to limit, stop, prevent and remediate such Incident. Following this initial notification, Acquia will promptly investigate the Security Incident and take all reasonable and necessary steps to prevent any further compromise of the Customer Data. If a security deficiency is identified within any Acquia information system during this investigation, Acquia will provide a report to Customer containing a description of the nature of the Security Incident, an identification of any Customer Data that was disclosed, destroyed, altered, or compromised, and any investigative, corrective, or remedial actions taken or planned by Acquia to mitigate the risk of further Security Incidents. Acquia will maintain log files sufficient to enable Customer to determine what Customer Data was accessed and when, regardless of whether such data is physically or electronically maintained.

11. Business Continuity and Disaster Recovery.

Acquia maintains business continuity and disaster recovery planning processes to establish and maintain plans and procedures for the continuity, recovery and operation of information systems, processes and facilities that could impact the availability of Customer Data ("**BC/DR Plans**"). These BC/DR Plans include processes for responding to emergencies (e.g., natural disasters such as fire, earthquakes, or hurricanes, or other disasters such as sabotage, virus, and terrorism), and includes: (i) descriptions of roles and responsibilities: identifying key individuals and the recovery team responsible for implementing recovery actions; (ii) data backup plans, providing for periodic backups of data from database systems that can be used to reconstruct data; (iii) contingency plans and disaster recovery guides that will be followed by members of the recovery team before, during and after an unplanned disruptive event in order to minimize downtime and data loss; and (iv) procedures for annual testing and evaluating the BC/DR Plans including documenting the tests in writing.

12. Security Evaluations.

a. Acquia performs periodic risk assessments that evaluate and assess the security of the system's physical configuration and environment, software, information handling processes, and user practices including appropriate logs and reports on security activity.

b. In addition, security policies are regularly reviewed and evaluated to ensure operational effectiveness, compliance with applicable laws and regulations, and to address new threats and risks.

c. Security Policies are also reviewed when there is a material change in Acquia's business practices or the external threat environment that may reasonably implicate the security or integrity of records containing Customer Data. Acquia uses a documented change control process for software, systems, applications, and databases that ensures access changes are controlled, approved, and recorded.

d. Acquia will promptly notify Customer of any planned system configuration changes or other changes that would adversely affect the confidentiality, integrity, or availability of Customer Data.

13. Acquia Certifications and Standards by Product Offering

Acquia engages reputable third-party, independent, audit firms to conduct the below audit engagements:

Acquia Offering	**Completed Certifications and Attestations**

Drupal Cloud ❖ Acquia Cloud Platform[4] ❖ Acquia Cloud Site Factory	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • CSA STAR • HIPAA[1] • PCI-DSS[2] • FedRAMP[3] • IRAP
Marketing Cloud ❖ Customer Data Platform ❖ Campaign Studio ❖ Campaign Factory ❖ Personalization	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • CSA CAIQ - CDP • HIPAA
Content Cloud ❖ Acquia DAM	• ISO 27001:2013 • CSA CAIQ

[1] HIPAA compliant indicates that the service can be used in a way that enables Customers to help meet its legal obligations for HIPAA compliance. Ultimately, Customers are responsible for ensuring compliance with legal obligations, that the Acquia service meets their compliance requirements, and that they secure the service appropriately. Customers can reference Acquia's SOC 2 report, which contains a matrix mapping HIPAA controls to Acquia's SOC 2 controls.

[2] PCI-DSS compliance requires the purchase of Acquia's PCI Cloud configuration within Acquia Cloud Enterprise and Acquia Cloud Site Factory.

[3] Federal Risk and Authorization Management Program ("FedRAMP") is available for select Customers (i.e. Federal Agency cloud deployments). Acquia's FedRAMP implementation is more fully described in its FedRAMP package, available via the OMB MAX repository system.

[4] Acquia Cloud Next (ACN) certification/attestations consist of ISO 27001:2013 and SOC 2 Type 1 (security, Availability, and Confidentiality). For additional detail concerning ACN compliance certification status please see https://docs.acquia.com/guide.

Acquia will provide copies of available audit reports for the applicable Services to Customers upon written request and under NDA. Such audit reports, and the information they contain, are Acquia Confidential Information and must be handled by Customer accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to the Services and are provided without any warranty. Acquia can also provide summary level penetration test documentation available to Customers upon request sanitized of any sensitive information.

14. Training and Secure Development Practices.

The Acquia Information Security Policy is communicated to all Acquia personnel, employees, and contractors. Acquia provides periodic and mandatory security awareness training to employees and contractors (collectively "**Personnel**"). Acquia imposes disciplinary measures for violations of the Acquia Information Security Policy:

Agreements with relevant Sub-processors include requirements that these Sub-processors address security risks, controls, and procedures for information systems and contain terms, conditions, and restrictions at least as protective and as restrictive as those set forth herein. Acquia shall supply each of its personnel and contractors with appropriate, ongoing training regarding information security procedures, risks, and threats and Acquia shall be responsible for the performance of any subcontractor. Acquia agrees that any Services performed for Customer involving use of Customer Data shall be performed only at the Data Center Region and by personnel permitted under the Agreement.

15. Acquia Shared Responsibility Model.

Acquia Responsibilities

Acquia is responsible for the confidentiality, integrity, and availability (the "**Security**") of the Services and internal Acquia information technology systems. In addition to those measures detailed in "Security of Data Processing" above, Security Measures include, but are not limited to, server-level patching, vulnerability management, penetration testing, security event logging & monitoring, incident management, operational monitoring, 24/7 support, and ensuring customer site availability in accordance with the applicable SLA.

Acquia uses Sub-processors for the Services and to support Acquia as a Processor of Customer data. Acquia shall remain fully liable for their acts and omissions relating to the performance of the respective Services and shall be responsible for ensuring that obligations under this Security Annex and the Agreement are carried out in accordance with both.

Customer Responsibilities

The Customer is responsible for the security of their Customer Application(s), as applicable. For example, patching the open-source software Drupal, that are used in conjunction with the Services. This includes, but is not limited to, ensuring a secure configuration and coding of the applications, related application security monitoring activities, Customer user access management, password configurations, implementing multi-factor authentication, periodic penetration testing, appropriate Application-level DoS or DDoS protections, and/or vulnerability scanning of their applications, amongst others.

In addition, Customers are also responsible for the secure management of their users and provision of users for the purpose of granting access to Acquia's Services and abiding by the Subscription and Services Agreement, the Data Processing Agreement and Acquia's Acceptable Use Policy in using Acquia's Services.

16. Access and Review.

Acquia will make summary level information regarding its security policies and procedures as well current, published, third-party audit reporting related to Customer's Customer Data available for Customer's review at Acquia upon reasonable prior written notice by Customer and subject to Acquia's confidentiality and security conditions, and subject to a written and mutually agreed audit plan. Acquia reserves the right to require its prior approval to any third-party review of the DR Plan, and reasonably condition and restrict such third-party access. As illustrated in, "Acquia Certifications and Standards by Product Offering" Customers may also review available audit reporting as outlined in Section 13.

17. Customer Audits.

Acquia offers its Services in the cloud in a one-to-many business model that relies on standardization of best practices and industry standards for the benefit of its Customers and which is utilizing third-party providers and Sub-processors. As a result, onsite audits by Customers pose security and privacy risks to Acquia, other Acquia Customers and Acquia Sub-processors.

Moreover, some Sub-processors such as Amazon Web Services ("**AWS**") do not allow for physical audits of their data centers, but instead provide third party audits and certifications. It is for these reasons, among others, that Acquia's security program consists of the audits, certifications and available documentation detailed in Section 13 "Acquia Certifications and Standards by Product Offering" above as part of balancing transparency regarding the security and privacy safeguards that Acquia has implemented, while also satisfying security and privacy requirements as part of security and privacy obligations to Acquia Customers, and its Sub-processors, including AWS.

Therefore, Customer agrees to exercise its right to conduct an audit or inspection of Acquia's processing of personal data within Customer Data by instructing Acquia to carry out audits as described above in Section 13 "Acquia Certifications and Standards by Product Offering" above using its current processes and timing. If Customer wishes to change this instruction regarding the audit or inspection, then Customer shall send such request by written notice to Acquia, and the parties agree to jointly discuss how to implement the changed instruction.

Exhibit 2
EU SCCs (Standard Contractual Clauses 2021) Annexes I and II

ANNEX I

LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: Customer per page above and any Customer Affiliates as further described in the DPA and Agreement

Address: per page above or as further described in the DPA and Agreement

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses: Use of the Services as procured by the Data exporter(s) from the Data importer(s) as further defined in the DPA and the Agreement.

Signature and date: per execution on page above

Role (controller/processor): Controller (or Processor on behalf of a third-party Controller)

2. _____

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

1. **Name**: Acquia Inc.

Address: 53 State Street, Boston, MA 02109, USA

Contact person's name, position and contact details: Stephan Dobrowolski, Assoc. General Counsel / Global Privacy Officer, privacy@acquia.com

Activities relevant to the data transferred under these Clauses: Provision of the Services as procured by the Data exporter(s) from the Data importer(s) as further defined in the DPA and the Agreement.

Signature and date: Per execution on page

Role (controller/processor): Processor.

2. The Acquia Affiliates as set out at: https://www.acquia.com/about-us/legal/subprocessors

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Categories of personal data transferred

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Sensitive data transferred (if applicable) and **applied restrictions or safeguards** that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

The **frequency of the transfer** (e.g., whether the data is transferred on a one-off or continuous basis).

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Nature of the processing

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Purpose(s) of the data transfer and further processing

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

The **period for which the personal data will be retained**, or, if that is not possible, the criteria used to determine that period

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

For **transfers to (sub-) processors**, also specify subject matter, nature and duration of the processing

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ in connection with the relevant information regarding sub-processors set out at https://www.acquia.com/about-us/legal/subprocessors

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the EU GDPR applies directly:	the competent supervisory authority determined in accordance with Clause 13 of the EU SCCs, and
Where the Swiss GDPR applies:	Federal Data Protection and Information Commissioner of Switzerland

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

- see the relevant Product Notice available online at https://docs.acquia.com/guide/ (marked as "**GDPR Product Notice"** or "**Privacy Product Notice**"), and
- see the Acquia Security Annex available online at https://www.acquia.com/sites/default/files/legal/acquia-security-annex.pdf (the version applicable as of signature of this DPA is attached hereto as **Exhibit 1**)

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Acquia requires its sub-processors to adhere to technical and organizational measures which are at least as equivalent as those referenced in the Acquia Security Annex (see **Exhibit 1** to the DPA).

Exhibit 3
Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

TABLE 1: PARTIES

Start date	from the date of last signature on page of this DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: per page above Trading name (if different): per page above Main address (if a company registered address): per page above Official registration number (if any) (company number or similar identifier): per page above	Full legal name: Acquia Inc. Trading name (if different): n/a Main address (if a company registered address): 53 State Street, Boston, MA 02109, USA Official registration number (if any) (company number or similar identifier): US Federal Tax ID (FEIN): 26-0493001
Key Contact	Full Name (optional): _____ Job Title: _____ Contact details including email: _____	Full Name (optional): n/a Job Title: Acquia Privacy Team Contact details including email: privacy@acquia.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: per page above Reference (if any): Exhibit 2 of the DPA to which this Exhibit 3 is attached Other identifier (if any): n/a Or

	☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	n/a	n/a	n/a	n/a	n/a	n/a
2	yes	yes	no option	General Authorisation	30 days	see the relevant Product Notice available online at https://docs.acquia.com/guide/ (marked as "GDPR Product Notice" or "Privacy Product Notice")
3	yes	yes	no option	General Authorisation	30 days	see the relevant Product Notice available online at https://docs.acquia.com/guide/ (marked as "GDPR Product Notice" or "Privacy Product Notice")
4	n/a	n/a	n/a	n/a	n/a	n/a

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:	Exhibit 2 Annex I to the DPA
Annex 1B: Description of Transfer:	Exhibit 2 Annex I to the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	Exhibit 2 Annex II to the DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	https://www.acquia.com/about-us/legal/subprocessors

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses[3]

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

[3] Alternative Part 2 Mandatory Clauses chosen.

ACQUIA SECURITY ANNEX

This Acquia Security Annex (the "Annex") supplements (1) the Acquia Subscription and Services Agreement or the terms of services agreement existing between the parties (the "**Agreement**"), and (2), if applicable, any data processing agreement existing between both parties (the "**DPA**").

Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the Agreement or DPA. In case of a conflict between this Annex, the Agreement, or DPA, the conflict shall be resolved by the following order of precedence: (1) DPA, (2) Agreement, (3) Annex.

1. Security Policy.

Acquia maintains a company-wide information security management system and control program that includes written security policies, standards and procedures based upon ISO/IEC 27001:2013 (collectively, the "**Acquia Information Security Policy**"). The Acquia Information Security Policy requires adherence to the following security principles (individually and collectively "Security Principle(s)"):

a. The identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of Customer Data to the extent that such Customer Data is provided to Acquia and maintained or processed by Acquia during its provision of Services by utilizing key operations and security practices such as:
   i. Secure software development practices;
   ii. Secure operating procedures and vulnerability management;
   iii. Ongoing employee training;
   iv. Controlling physical and electronic access to Customer Data, and
   v. Means for detecting and preventing intrusions and security system failures on critical systems.

b. That Acquia follow the Security Principle of least privilege access, allowing only active Acquia employees and contractors access to records containing Customer Data and limit such access to those persons who are reasonably required to know such information in order to accomplish a valid business purpose or to comply with record retention regulations;

c. That Customer Data that is identified as such to Acquia by the customer at intake, is secured appropriately commensurate to the nature of Customer Data, including any individual personal data provided to Acquia by Customer as set forth in this Annex, using commercially available and industry accepted controls and precautionary measures;

d. That commercially reasonable standards are followed with respect to strong change-control procedures and technical controls that enforce segregation of duties, minimum necessary dataset, and access controls;

e. Monitoring of operations and maintaining procedures to ensure that security protocols are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Customer Data, and continuously improving information safeguards as necessary to mitigate risks;

f. A security patch and vulnerability management process based on accepted industry standard practices and protocols, including, monitoring threats, and responding to vulnerabilities reported by third parties; and

g. A security incident response and disaster recovery planning, including documentation of responsive actions taken in connection with any security incident related to Customer Data.

2. Security Practices and Processes.

a. Customers are responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any Customer Data processed, stored, or transmitted through the Subscription Services for which regulations other than those set forth in this Annex apply. If, while providing Subscription Services, Acquia agrees in writing to process such Customer Data and Customer has subscribed to any applicable Subscription Services, Acquia shall process it only as permitted under this Agreement and in compliance with the DPA and applicable data protection legislation to which Acquia is subject as a service provider. If Acquia agrees to receive Customer Data from Customer, Acquia will manage and/or process such Customer Data pursuant to the security requirements, obligations, specifications and event reporting procedures as set forth in this Annex, the DPA, and the Agreement, and any amendments thereto.

b. Acquia will comply with secure software development practices consistent with industry accepted standards and practices.

c. Acquia restricts access to Customer Data and systems by users, applications, and other systems. These controls include (i) controls to systems and data, limited to properly authenticated and authorized individuals based on principles of least privilege and need-to-know; and (ii) physical access controls, as described below. Acquia will limit access to Customer Data to the minimum necessary dataset required in order to perform the relevant Service(s).

d. Acquia shall comply with the Acquia Physical Security Policy, as may be updated from time to time, and which shall include access and asset management controls (e.g., electronic locks, access badges, and video surveillance) that provide a physically secure environment.

e. Acquia logs access to controlled systems and records, including successful and failed system access attempts, and restricts the connection times of users. Acquia will use unique logins on all network equipment, whenever commercially reasonable.

f. Acquia maintains processes to identify and deploy security patches in a timely manner. Unless otherwise expressly agreed in writing, "timely" means that Acquia will introduce a fix or patch as soon as commercially reasonable after Acquia becomes aware of the security problem or availability of a fix or patch.

3. Patch and Vulnerability Management.

a. Acquia follows commercially reasonable best practices for centralized patch management, criticality ranking and patching time frame requirements for all Acquia-operated systems, switches, routers, appliances, servers, and workstation PC's, as applicable.

b. Where feasible, Acquia ensures that trusted, commercially available anti-virus software is installed, enabled, and kept current on Acquia servers and systems used in accessing, processing, transmitting, or storing Customer Data.

c. Acquia maintains trusted, current, commercially available anti-malware protection capabilities on Acquia devices, particularly those used for accessing, processing, transmitting, or storing Customer Data.

d. Acquia maintains a vulnerability management solution for devices connected to Acquia's LAN. Such solution is designed to regularly assess Acquia's network for known vulnerabilities.

4. Security Monitoring.

a. Acquia has a designated security team which monitors Acquia's control environment which is designed to prevent unauthorized access to or modification of Acquia's Customer Data. Acquia regularly monitors controls of critical systems, network, and procedures to validate proper implementation and effectiveness in addressing the threats, vulnerabilities and risks identified. This monitoring is variable by the criticality, exposure, and the system's assets and may include: (i) internal risk assessments; (ii) validation of Multi-Factor Authentication for select environments; (iii) third party compliance, including hosting services and third-party components; and (iv) assessing changes affecting systems processing authentications, authorizations, and auditing.

b. Acquia performs periodic vulnerability assessments on Acquia applications and systems. Penetration tests are performed either by Acquia or by an established, reputable independent third party.

5. Security of Data Processing.

Acquia has implemented and will maintain technical and organizational measures inclusive of administrative, technical, and physical safeguards to ensure a level of security appropriate to the risk of the data processing for the Acquia Services as described in this Annex (the "Security Measures"). These Security Measures may be changed by Acquia from time to time during the Term of the Agreement to take into account advancements in available security technologies. However, Acquia will not materially decrease the overall security of the Services during a Subscription Term.

The Security Measures may include, but will not be limited to, the following measures for ensuring the ongoing confidentiality, integrity, and availability of Customer Data to prevent unauthorized access, use, modification or disclosure of Customer Data:

b. Background Checks.

Performance of background checks on all personnel, as well as execution of non-disclosure commitments prior to employment and acknowledgment of professional behavior in the workplace documents, which includes anti-harassment and code of business conduct and ethics.

c. Training.

Security and privacy awareness training, inclusive of acknowledgment and agreement to abide by organizational security policies, for all personnel upon hire and annually thereafter.

d. Customer Data.

Pseudonymization or encryption of Customer Data in transit and at rest utilizing industry-standard mechanisms for certain Acquia Services.

A process for regularly testing, assessing and evaluating the effectiveness of administrative, technical and physical safeguards for ensuring the security of the processing, transmission or storage of Customer Data through external and internal audits as further described below.

Preventing access, use, modification, or disclosure of Customer Data except by authorized Acquia personnel (1) to provide the Subscription Services and prevent or address service or technical problems, (2) as compelled by law, or (3) as Customer expressly permits in writing; in any event pursuant to the terms set forth in an applicable DPA.

e. Availability.

The ability to restore the availability and access to Customer Data in a timely manner in the event of an incident impacting the availability of the Services by maintaining a backup solution for disaster recovery purposes.

f. Logging and Monitoring.

Logging and monitoring of security logs via a Security Incident Event Management ("**SIEM**") system and alerting to a dedicated Incident Response team upon the detection of suspicious system and/or user behaviors.

g. Vulnerability Triaging.

Processes and tooling for regularly identifying, assessing and triaging vulnerabilities based on industry-standard guidelines.

h. Policies

Maintenance of a comprehensive set of security and privacy policies, procedures and plans that are reviewed on at least an annual basis and provide guidance to the organization regarding security and privacy practices; and,

i. Sub-processors.

Processes for evaluating prospective and existing Sub-processors to ensure that they have the ability and commit to appropriate administrative, technical and physical measures to ensure the ongoing confidentiality, integrity and availability of Customer Data.

By implementing the Security Measures detailed above Acquia, considers the risks that are related to data processing, in particular the ones resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

6. Secure Data Transmissions.

Any Customer Data that Acquia transmits over a public communications network will be protected during transmission by using, or making available, industry accepted standards such as TLS, SSH and VPNs.

7. Data and Media Disposal.

Acquia maintains procedures that align with industry standards, such as NIST SP 800-88, regarding the disposal of both tangible property and electronic files containing Customer Data, considering available technology so that Customer Data cannot be reconstructed and read.

8. Backup and Retention.

Acquia will backup systems used to provide services to Customer to ensure adequate recovery capabilities in accordance with the schedule set forth in the Documentation for the applicable Services. Back-ups will be appropriately protected to ensure only authorized individuals are able to access the Customer Data, including but not limited to encryption of data stored off-site in electronic media and appropriate classification and protection of hard copy records, as applicable. If not separately backed up, Acquia will secure any files containing Customer Data against unauthorized access in accordance with the terms of the Agreement.

9. Customer Data.

Acquia will comply with those laws and regulations applicable to the provision of the Services concerning the confidentiality, security, and processing of any Customer Data that it receives from Customer. In the event Acquia processes types of Customer Data that are subject to additional regulatory requirements due to the nature of the data or its place of origin (as defined in section 2a above) Acquia will reasonably cooperate with Customer to arrange compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g. EU Standard Contractual Clauses, Business Associate Agreement governing Protected Health Information), implementation of additional security controls required by such law, completion of regulatory filings applicable to Acquia, and participation in relevant regulatory audits as applicable from Section 17 below ("Customer Audits.").

10. Security Incident Management and Remediation.

For purposes of this Annex, a "**Security Incident**" means (i) the loss of, (ii) unauthorized acquisition, use or disclosure of, or (iii) unauthorized access to, Customer Data resulting from a security breach of the Acquia platform. Acquia maintains a response function capable of identifying and assessing the seriousness and extent of a Security Incident, mitigating the effect of a Security Incident, conducting root cause analysis, implementing, and documenting remedial action plans, and preventing the recurrence of Security Incidents. Acquia has an established set of procedures to ensure personnel and contractors promptly report actual and/or suspected breaches of security. Acquia keeps an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents, as well as performing required recovery actions to remedy the impact.

a. Security Incidents on Acquia's platform are logged and reviewed, secured, and retained as required by applicable laws and regulations.

b. In the case of a Security Incident that relates to Customer Data, Acquia shall (a) promptly assess and contain such Security Incident, (b) notify Customer, without undue delay, upon becoming aware of such Incident, and in no case later than forty-eight (48) hours after Acquia has become aware of such Security Incident, via a Support ticket to each of the individuals

identified by Customer for distribution of such Support Tickets (or such other addresses as may be provided by Customer from time to time) and provide regular status updates to Customer regarding the investigation at a frequency reasonably requested by Customer depending upon the severity of such Incident, (c) as applicable, provide reasonable cooperation and assistance to Customer needed to fulfill Customer's obligations related to Customer's use of the Services, as applicable, and (d) immediately take all steps reasonably necessary and within Acquia's reasonable control, including without limitation, those reasonably requested by Customer, to limit, stop, prevent and remediate such Incident. Following this initial notification, Acquia will promptly investigate the Security Incident and take all reasonable and necessary steps to prevent any further compromise of the Customer Data. If a security deficiency is identified within any Acquia information system during this investigation, Acquia will provide a report to Customer containing a description of the nature of the Security Incident, an identification of any Customer Data that was disclosed, destroyed, altered, or compromised, and any investigative, corrective, or remedial actions taken or planned by Acquia to mitigate the risk of further Security Incidents. Acquia will maintain log files sufficient to enable Customer to determine what Customer Data was accessed and when, regardless of whether such data is physically or electronically maintained.

11. Business Continuity and Disaster Recovery.

Acquia maintains business continuity and disaster recovery planning processes to establish and maintain plans and procedures for the continuity, recovery and operation of information systems, processes and facilities that could impact the availability of Customer Data ("**BC/DR Plans**"). These BC/DR Plans include processes for responding to emergencies (e.g., natural disasters such as fire, earthquakes, or hurricanes, or other disasters such as sabotage, virus, and terrorism), and includes: (i) descriptions of roles and responsibilities: identifying key individuals and the recovery team responsible for implementing recovery actions; (ii) data backup plans, providing for periodic backups of data from database systems that can be used to reconstruct data; (iii) contingency plans and disaster recovery guides that will be followed by members of the recovery team before, during and after an unplanned disruptive event in order to minimize downtime and data loss; and (iv) procedures for annual testing and evaluating the BC/DR Plans including documenting the tests in writing.

12. Security Evaluations.

a. Acquia performs periodic risk assessments that evaluate and assess the security of the system's physical configuration and environment, software, information handling processes, and user practices including appropriate logs and reports on security activity.

b. In addition, security policies are regularly reviewed and evaluated to ensure operational effectiveness, compliance with applicable laws and regulations, and to address new threats and risks.

c. Security Policies are also reviewed when there is a material change in Acquia's business practices or the external threat environment that may reasonably implicate the security or integrity of records containing Customer Data. Acquia uses a documented change control process for software, systems, applications, and databases that ensures access changes are controlled, approved, and recorded.

d. Acquia will promptly notify Customer of any planned system configuration changes or other changes that would adversely affect the confidentiality, integrity, or availability of Customer Data.

13. Acquia Certifications and Standards by Product Offering

Acquia engages reputable third-party, independent, audit firms to conduct the below audit engagements:

Acquia Offering	Completed Certifications and Attestations
Drupal Cloud ❖ Acquia Cloud Platform[4] ❖ Acquia Cloud Site Factory	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2022 • CSA STAR • HIPAA[1] • PCI-DSS[2] • FedRAMP[3] • IRAP5
Marketing Cloud ❖ Customer Data Platform ❖ Campaign Studio ❖ Campaign Factory ❖ Personalization	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2022 • CSA STAR • HIPAA1

Content Cloud
❖ Acquia DAM
	• ISO 27001:2022
	• CSA STAR
	• HIPAA1
	  • SOC 1 Type 2 (SSAE18 & ISAE 3402)
	  • SOC 2 Type 2 (Security, Availability and Confidentiality)

[1] HIPAA ready indicates that the service can be used in a way that enables Customers to help meet its legal obligations for HIPAA compliance , including Acquia entering into a Business Associate Agreement (BAA) for the identified services. Ultimately, Customers are responsible for ensuring compliance with legal obligations, that the Acquia service meets their compliance requirements, and that they secure the service appropriately. Customers can reference Acquia's SOC 2 report, which contains a matrix mapping HIPAA controls to Acquia's SOC 2 controls.

[2] PCI-DSS compliance requires the purchase of Acquia's PCI Cloud configuration within Acquia Cloud Enterprise and Acquia Cloud Site Factory.

[3] Federal Risk and Authorization Management Program ("FedRAMP") is available for select Customers (i.e. Federal Agency cloud deployments). Acquia's FedRAMP implementation is more fully described in its FedRAMP package, available via the USDA Connect repository system.

[4] Acquia Cloud Next (ACN) is included within the scope of the definition of Acquia Cloud Platform.

5 The Information Security Registered Assessor Program (IRAP) is available for select Customers (i.e. Australian government cloud deployments). Acquia's IRAP implementation is more fully described in its IRAP package, available upon request where authorized.

Acquia will provide copies of available audit reports for the applicable Services to Customers upon written request and under NDA via https://security.acquia.com. Such audit reports, and the information they contain, are Acquia Confidential Information and must be handled by Customer accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to the Services and are provided without any warranty. Acquia can also provide summary level penetration test documentation available to Customers upon request sanitized of any sensitive information.

14. Training and Secure Development Practices.

The Acquia Information Security Policy is communicated to all Acquia personnel, employees, and contractors. Acquia provides periodic and mandatory security awareness training to employees and contractors (collectively "**Personnel**"). Acquia imposes disciplinary measures for violations of the Acquia Information Security Policy:

Agreements with relevant Sub-processors include requirements that these Sub-processors address security risks, controls, and procedures for information systems and contain terms, conditions, and restrictions at least as protective and as restrictive as those set forth herein. Acquia shall supply each of its personnel and contractors with appropriate, ongoing training regarding information security procedures, risks, and threats and Acquia shall be responsible for the performance of any subcontractor. Acquia agrees that any Services performed for Customer involving use of Customer Data shall be performed only at the Data Center Region and by personnel permitted under the Agreement.

15. Acquia Shared Responsibility Model.

Acquia Responsibilities

Acquia is responsible for the confidentiality, integrity, and availability (the "**Security**") of the Services and internal Acquia information technology systems. In addition to those measures detailed in "Security of Data Processing" above, Security Measures include, but are not limited to, server-level patching, vulnerability management, penetration testing, security event logging & monitoring, incident management, operational monitoring, 24/7 support, and ensuring customer site availability in accordance with the applicable SLA.

Acquia uses Sub-processors for the Services and to support Acquia as a Processor of Customer data. Acquia shall remain fully liable for their acts and omissions relating to the performance of the respective Services and shall be responsible for ensuring that obligations under this Security Annex and the Agreement are carried out in accordance with both.

Customer Responsibilities

The Customer is responsible for the security of their Customer Application(s), as applicable. For example, patching the open-source software Drupal, that are used in conjunction with the Services. This includes, but is not limited to, ensuring a secure configuration and coding of the applications, related application security monitoring activities, Customer user access management, password configurations, implementing multi-factor authentication, periodic penetration testing, appropriate Application-level DoS or DDoS protections, and/or vulnerability scanning of their applications, amongst others.

In addition, Customers are also responsible for the secure management of their users and provision of users for the purpose of granting access to Acquia's Services and abiding by the Subscription and Services Agreement, the Data Processing Agreement and Acquia's Acceptable Use Policy in using Acquia's Services.

16. Access and Review.

Acquia will make summary level information regarding its security policies and procedures as well current, published, third-party audit reporting related to Customer's Customer Data available for Customer's review at Acquia upon reasonable prior written notice by Customer and subject to Acquia's confidentiality and security conditions, and subject to a written and mutually agreed audit plan. Acquia reserves the right to require its prior approval to any third-party review of the DR Plan, and reasonably condition and restrict such third-party access. As illustrated in, "Acquia Certifications and Standards by Product Offering" Customers may also review available audit reporting as outlined in Section 13.

17. Customer Audits.

Acquia offers its Services in the cloud in a one-to-many business model that relies on standardization of best practices and industry standards for the benefit of its Customers and which is utilizing third-party providers and Sub-processors. As a result, onsite audits by Customers pose security and privacy risks to Acquia, other Acquia Customers and Acquia Sub-processors.

Moreover, some Sub-processors such as Amazon Web Services ("**AWS**") do not allow for physical audits of their data centers, but instead provide third party audits and certifications. It is for these reasons, among others, that Acquia's security program consists of the audits, certifications and available documentation detailed in Section 13 "Acquia Certifications and Standards by Product Offering" above as part of balancing transparency regarding the security and privacy safeguards that Acquia has implemented, while also satisfying security and privacy requirements as part of security and privacy obligations to Acquia Customers, and its Sub-processors, including AWS.

Therefore, Customer agrees to exercise its right to conduct an audit or inspection of Acquia's processing of personal data within Customer Data by instructing Acquia to carry out audits as described above in Section 13 "Acquia Certifications and Standards by Product Offering" above using its current processes and timing. If Customer wishes to change this instruction regarding the audit or inspection, then Customer shall send such request by written notice to Acquia, and the parties agree to jointly discuss how to implement the changed instruction.

DISCLAIMER: INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.