SUBSCRIPTION AND SERVICES AGREEMENT

This subscription and services agreement (the "**Agreement**"), the relevant terms of the Documentation, and any executed Orders and/or SOWs between the parties, are incorporated herein and shall govern the provision of the Services. Customer and its Affiliates may place orders under this Agreement by submitting separate Order(s) and SOW(s). This Agreement shall commence on the Effective Date of Customer's first executed Order or SOW ("**Effective Date**") and will continue until otherwise terminated in accordance with Section 12 below.

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.

"**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, that are submitted, stored, posted, displayed, transmitted, or otherwise used by or for Customer to 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 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 Marketplace" means any non-Acquia products or services made available as an accommodation through Acquia's website, which are subject to change during the Subscription Term.

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.

2.3. Third Party Marketplace. As part of the Subscription Services, Acquia may provide access to the Third Party Marketplace solely as an accommodation to Customer. Customer may choose to use any, all or none of the offerings on such Third Party Marketplace at its sole discretion. Customer's use of any offering on the Third Party Marketplace 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 Marketplace products and services.

2.4 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. In performing the Subscription Services, Acquia will comply with the Acquia Privacy Policy attached hereto and incorporated herein by reference. The Acquia Privacy Policy is subject to change at Acquia's discretion; however, Acquia policy changes will not result in a material reduction in the level of protection provided for Customer Data during the Subscription Term. Except with respect to Trial Services, the terms of the Acquia GDPR Data Processing Addendum ("DPA") are attached hereto and hereby incorporated by reference and shall apply to the extent Customer Data includes Personal Data, as defined in the DPA. 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 regulation 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. 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, and its implementing regulations, as amended or superseded from time to time ("CCPA"), such data processing by Acquia as a "service provider" complies with the requirements of the CCPA. 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 is not generally applicable to information technology services providers.

4. CUSTOMER OBLIGATIONS

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.

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 and SOW and any applicable additional fees if Customer exceeds the allotted capacity or other applicable limits specified in the Order. Except as otherwise specified herein or in an Order or SOW (i) fees are payable in United States dollars, (ii) fees are based on Services purchased, regardless of usage, (iii) except as expressly stated herein payment obligations are non-cancelable and fees paid are non-refundable, , (iv) all Services shall be deemed accepted upon delivery, and (v) the Subscription Services purchased cannot be decreased during the relevant Subscription Term. Customer shall reimburse Acquia in accordance with Federal Travel Regulation (FTR)/Joint Travel Regulations (JTR), as applicable for travel expenses incurred by Acquia in connection with its performance of Services . Acquia will provide Customer with reasonably detailed invoices for such expenses Customer shall only be liable for such travel expenses as approved by Customer and funded under the applicable ordering document. All amounts payable under this Agreement will be made without setoff or counterclaim, and without any deduction or withholding.

6.2. Invoicing and Payment. Unless otherwise specified in an Order, fees for Subscription Services specified in an Order will be invoiced annually at the time of purchase, fees for overages will be calculated and invoiced monthly in arrears, and, unless otherwise set forth in an SOW, all fees and expenses for standard Professional Services as described in Section 5.1 shall be invoiced 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; provided that Acquia will not exercise its right to charge interest if the applicable charges are under reasonable and good faith dispute and Customer is cooperating diligently to resolve the issue.

6.3. Taxes. Fees for Services exclude all sales, value added and other taxes and duties imposed with respect to the sale, delivery, or use of any product or Services covered hereby. Unless Customer provides a valid, signed certificate or letter of exemption for each respective jurisdiction of its tax-exempt status, Customer is responsible for payment of all taxes, levies, duties, assessments, including but not limited to value-added, sales, use or withholding taxes, assessed or collected by any governmental body (collectively, "**Taxes**") arising from Acquia's provision of the Services hereunder, except any taxes assessed on Acquia's net income. If Acquia is required to directly pay or collect Taxes related to Customer's use or receipt of the Services hereunder, Customer agrees to promptly reimburse Acquia for any amounts paid by Acquia Acquia 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), or else a valid, signed certificate or letter of exemption for each respective jurisdiction of its tax- exempt status, as appropriate.

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 Software. 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 Software**"). Such Third Party Software is provided to the Customer without liability or obligation by Acquia and is governed by a license agreement directly between the Customer and the respective owner of the Third Party Software. Such license agreement may be found in the relevant section of the user interface subdirectory available through the Documentation.

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 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 the terms and conditions of this Agreement (to the extent permitted under applicable law, pricing and other terms set forth in all Order Forms and/or SOWs hereunder)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, 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.

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.

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 Acquia'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. Subscription Term. Each Subscription Term shall be set forth in the applicable Order. .

12.3. Termination. When the Customer is an instrumentality of the U.S. Government, 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. In no event shall any termination relieve Customer of the obligation to pay all fees payable to Acquia for the period prior to the effective date of termination. Upon termination of an Order Form or this Agreement for any reason, Customer's right to access and use the Subscription Services (including any Ancillary Programs) terminates. Upon such termination, Customer must (a) immediately destroy all copies of the Ancillary Programs, and (b) immediately and, upon Acquia's request, provide Acquia with written certification of such destruction.

12.4. When the Customer is NOT an instrumentality of the U.S. Government, A party may terminate this Agreement (or, at such party's option, the individual Order Forms or SOWs affected by the applicable breach), for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such same 30 day period, or (ii) automatically if the other party becomes the subject of a petition in bankruptcy or other proceeding relating to **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 (Refund upon Termination), 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 the United States. 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, 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. Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Order Forms and SOWs), without consent of the other party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor 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.

PRIVACY POLICY

Introduction

Acquia Inc., including its wholly owned affiliates, (“Acquia”, "us," "we," or "our,") is committed to protecting the privacy of your information. This Privacy Policy (“Policy”) governs Acquia’s use of personally identifiable information, also "personal data," about users of our products, services and/or software that are available for purchase and use through our sales teams, accessible by download on our websites (our "Services"), and also users of our website http://acquia.com as well as the other websites that Acquia operates and that link to this Policy (collectively referred to as “Site(s)”). It also describes the choices available to you regarding our use of your personally identifiable information and how you can access and update this information.

Acquia complies with the relevant regulation applying to personal data, including but not limited the General Data Protection Regulation issued by the European Union.

Our Sites may contain links to other websites, applications, and services maintained by third parties. The information practices of other services are governed by their privacy statements, which you should review to better understand their privacy practices.

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

Acquia complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the United States Department of Commerce regarding the collection, use, and retention of personally identifiable information transferred from the European Union, and the United Kingdom and/or Switzerland to the United States. Consistent with our commitment to protect personally identifiable information about individuals in the European Union, Acquia has certified to the Department of Commerce that it adheres to the Privacy Shield Principles of Notice, Choice, and Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability (the “Privacy Shield Principles” or the “Principles”). Acquia’s EU-U.S. and Swiss-U.S. Privacy Shield Certification also extends to personally identifiable information that we receive directly through the Sites. More information on the EU-U.S. and Swiss-U.S. Privacy Shield and Acquia’s scope of participation in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks are available at http://www.privacyshield.gov/welcome.

If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

California Residents

If you are a California consumer, for more information about your privacy rights, please see our California Consumer Privacy Statement.

Brazil Residents

If you are a Brazil consumer, for more information about your privacy rights under Lei Geral de Proteção de Dados Pessoais (“LGPD”), please contact us at Legal@acquia.com.

Privacy Policy Updates

Due to the Internet’s rapidly evolving nature, Acquia may need to update this Privacy Policy from time to time. If so, Acquia will post our updated Privacy Policy on our Site located at http://acquia.com/about-us/legal/privacy-policy and post notice of the change so it is visible when users log-on for the first time after the change is posted so that you are always aware of what personally identifiable information we may collect and how we may use this information. If we make material changes to this policy, we will notify you here, by email, or by means of a notice on our home page. Acquia encourages you to review this Privacy Policy regularly for any changes. Your continued use of this Site and/or continued provision of personally identifiable information to us will be subject to the terms of the then-current Privacy Policy.

Data Integrity and Purpose Limitation

Acquia is a provider of cloud platform related services, including Platform as a Service (“PaaS”) and Software as a Service (“SaaS”) products, technical support services and professional consulting services for Drupal websites which processes personally identifiable information upon the instruction of its customers in accordance with the terms of the applicable agreement between Acquia and customer.

Information Collection and Use

You can generally visit our Site without revealing any personally identifiable information about yourself. However, in certain sections of thes Site or interactions with us, we may invite you to participate in one or some of the following. We collect such information in the following situations:

Surveys (If you voluntarily submit certain information to our services, such as filling out a survey about your user experience, we collect the information you have provided as part of that request)

Contact Us features with questions or comments or request information, participate in chat or message boards (If you express an interest in obtaining additional information about our services, request customer support, use our “Contact Us” or similar features, register to use our services, sign up for an event, questionnaires, webinar, contests, or download certain content, we may require that you provide to us your contact information)

If you interact with our websites or emails, we may automatically collect information about your device and your usage of our websites or emails, (such as Internet Protocol (IP) addresses or other identifiers, which may qualify as Personal Data) (see “Device and Usage Data Processing section, below) using cookies, Web Beacons, or similar technologies.

If you make purchases via our Sites or register for an event or webinar, we may require that you provide your financial and billing information, such as billing name and address, credit card number or bank account information.

If you communicate with us via a phone call from us, we may record that call.

We require you to complete a registration form and/or create a profile to access certain restricted areas of the Site, to use certain services and when you download any software.

If you visit our offices, you may be required to register as a visitor and to provide your name, email address, phone number, company name, and time and date of arrival. Additionally, due to the COVID-19 pandemic, you may be required to provide information regarding your health status, including your temperature, COVID-19 related symptoms, exposure to COVID-19, positive individuals, and recent travel history.

Due to the nature of some of these activities, we may collect personally identifiable information such as your name, e-mail address, address, phone number, password, screen name, credit card information and other contact information that you voluntarily transmit with your on-line and in-person communications to us and personally identifiable information that you elect to include in your chart and message board postings.

If you use a forum on this Site, you should be aware that any personally identifiable information you submit there can be read, collected, or used by other users of these forums, and could be used to send you unsolicited messages. We are not responsible for the personally identifiable information you choose to submit in these forums. We receive permission to post testimonials that include personally identifiable information prior to posting.

If you provide us or our service providers with any Personal Data relating to other individuals, you represent that you have the authority to do so, and where required, have obtained the necessary consent, and acknowledge that it may be used in accordance with this Privacy Policy. If you believe that your Personal Data has been provided to us improperly, or want to exercise your rights relating to your Personal Data, please contact us by emailing privacy@acquia.com.

Orders

If you purchase a product or service from us, we request certain personally identifiable information from you on our order form. You must provide contact information (such as name, email, and shipping address) and financial information (such as credit card number, expiration date).

We use this information for billing purposes and to fill your orders. If we have trouble processing an order, we will use this information to contact you.

In addition, we may collect information about the performance, security, software configuration and availability of customer web sites in an automated fashion as part of the Acquia subscription services.

We use your personally identifiable information to register you to use our services or download or access software or other content, contact you to deliver certain goods, services or information that you have requested, provide you with notices regarding goods or services you have purchased, provide you with notices regarding goods or services that you may want to purchase in the future (including communications from third party service providers and/or Acquia technology partners concerning additional products/applications which compliment Acquia's services, or else are customizable with Acquia's services in order to maximize your digital experience while leveraging Acquia services), verify your authority to enter our Site and improve the content and general administration of the Site and our services.

Certain modules within the Drupal software connect your installation of Drupal to our subscription services, these modules will report to us, and we will collect, your IP address, operating system type and version, web server type and version, php version, database type and version, version of the services, modifications to your Drupal code, information regarding the availability of your website (e.g. if your website is live or down), website user statistics such as the number of nodes, number of users and number of comments. The foregoing information will be linked to your personally identifiable information and user accounts and we may use the foregoing information to better provide technical support to you and our customers and to improve our services.

If you install and use the Acquia Search module and connect your Drupal site to the subscription services, in addition to the information we may collect, analyze and store when you use our services as stated above, the Acquia Search module may collect, analyze and store the content of your site in an index. This index will be stored and updated on our servers to enable Acquia Search to work with your site. A copy of this index may be retained for up to 14 days as a backup in the event there is a problem with the index. Additionally, information about the size of your index, the search queries performed on your index, performance of Acquia Search for your queries, and other operational information is stored indefinitely in order to enable Acquia to monitor performance over time, manage the Search Service, and to provide you with information about the Search activity on your site.

If you choose to contact us by e-mail, we will not disclose your contact information contained in the e-mail, but we may use your contact information to send you a response to your message. Notwithstanding the foregoing, we may publicly disclose the content and/or subject matter of your message, therefore, you should not send us any ideas, suggestions or content that you consider proprietary or confidential. All e-mail content (except your contact information) will be treated on a non-proprietary and non-confidential basis and may be used by us for any purpose.

Details of data processing

Acquia processes your personal data as a customer and other customer’s personal data (in the following just “customer”) in order to provide the contractually agreed Services.

Subject matter: The subject matter of the data processing is the performance of the Services agreed between Acquia and customer by Acquia involving personal data provided by customer.

Duration: As between customer and Acquia, the duration of the data processing is determined by customer and its contractual commitments with regard to the use of Acquia’s Services.

Purpose: The purpose of the data processing by Acquia is the provision of the Services initiated by the customer from time to time.

Nature of the processing: Cloud computing as platform and software as a service and such other Services as described in the Documentation and initiated by the customer from time to time.

Type of personal data:

The type and extent of personal data that is subjected to Acquia’s data processing is determined and controlled by our customer as data controller in its sole discretion - this may include, but is not limited to the following:

First and last name

Title, work department, and manager/supervisor name

Position and employment history

Employer

Contact information (company, personal and work email, phone, home address, physical business address, emergency contact details)

Photographs

Biographical and directory information, including linked social media profile or posts

Company user names or IDs and login credentials

Identifiers related to work or personal devices used to access data exporter's IT systems

Log information generated through the use of data exporter's IT systems

Actions performed by the employee while accessing or using the Services

Full time or part time status

Business travel arrangements

Training undertaken and training needs

Localization data

Categories of data subjects: Customer's representatives and end-users including employees, contractors, collaborators and advisors of our customer (who are natural persons).

Communications from the Site

Special Offers and Updates

We will occasionally send you information on products, services, special deals, promotions. Out of respect for your privacy, we present the option not to receive these types of communications. Please see "Choice and Opt-out."

Newsletters

If you wish to subscribe to our newsletter(s), we will use your name and email address to send the newsletter to you. Out of respect for your privacy, we provide you a way to unsubscribe. Please see the "Choice and Opt-out" section.

Service-related Announcements

We will send you strictly service-related announcements on rare occasions when it is necessary to do so. For instance, if our service is temporarily suspended for maintenance, we might send you an email.

Generally, you may not opt-out of these communications, which are not promotional in nature. If you do not wish to receive them, you have the option to deactivate your account.

Customer Service

Based upon the personally identifiable information you provide us, we will send you a welcoming email to verify your username and password. We will also communicate with you in response to your inquiries, to provide the services you request, and to manage your account. We will communicate with you by email or telephone, in accordance with your wishes.

Choice/Opt-out

We or one of our authorized partners may place or read cookies on your device when you visit our websites for the purpose of serving you targeted advertising (also referred to as "online behavioral advertising" or "interest-based advertising"). To learn more about targeted advertising and advertising networks please visit the opt-out pages of the Network Advertising Initiative, here, and the Digital Advertising Alliance, here. We provide you the opportunity to 'opt-out' of having your personally identifiable information used for certain purposes, when we ask for your information.

To request updates or changes to your information or your preferences regarding receiving future promotional messages from us, you may contact our Privacy Officer using the information in the Contact Us section of this Privacy Policy or follow the opt-out instructions that are contained in the bottom of the email communication you received.

You will be notified prior to when your personally identifiable information is collected by any third party that is not our agent/service provider, so you can make an informed choice as to whether or not to share your information with that party.

Please note that if you opt out of receiving our promotional or marketing emails, you may still receive certain service-related communications from us, such as administrative and services announcements and messages about your account. Occasionally these materials are sent from a different email domain: marketing@theacquiateam.com.

Employment Opportunities

We provide you with a means for submitting your resume or other personally identifiable information through the Site for consideration for employment opportunities at Acquia. Personally identifiable information received through resume submissions will be kept confidential. We may contact you for additional information to supplement your resume, and we may use your personally identifiable information within Acquia, or keep it on file for future use, as we make our hiring decisions.

Children's Privacy

Acquia recognizes the privacy interests of children and we encourage parents and guardians to take an active role in their children's online activities and interests. This Site is not intended for children under the age of 13. Acquia does not target its services or this Site to children under 13. Acquia does not knowingly collect personally identifiable information from children under the age of 13. If you are a parent or guardian and believe your child has provided us with personal information without your consent, please contact us by emailing privacy@acquia.com.

Cookies and GIFs

We use small text files called cookies to improve overall Site experience. A cookie allows us to gather information about the use of our sites and how people interact with our emails. Cookies generally do not permit us to personally identify you (except as provided below). We may also use clear GIFs (a.k.a. "Web beacons") in HTML-based emails sent to our users to track which emails are opened by recipients.

Additionally, when using the Site, we and any of our third party service providers may use cookies and other tracking mechanisms to track your user activity on the Site and identify the organization or entity from which you are using the Site. If you register with the Site, we, and our third party service providers, will be able to associate all of your user activity with your personally identifiable registration information. We will use such user activity information to improve the Site, to provide context for our sales and support staff when interacting with you and customers, to initiate automated email marketing campaigns triggered by your activity on the Site and for other internal business analysis.

Aggregate Information

The Site may track information that will be maintained, used and disclosed in aggregate form only and which will not contain your personally identifiable information, for example, without limitation, the total number of visitors to our Site, the number of visitors to each page of our Site, browser type, External Web Sites (defined below) linked to and IP addresses. We may analyze this data for trends and statistics in the aggregate, and we may use such aggregate information to administer the Site, track users' movement, and gather broad demographic information for aggregate use.

Disclosure

We will not sell your personally identifiable information to any company or organization, except we may transfer your personally identifiable information to a successor entity upon a merger, consolidation or other corporate reorganization in which Acquia participates or to a purchaser or acquirer of all or substantially all of Acquia's assets to which this Site relates. We may provide your personally identifiable information and the data generated by cookies and the aggregate information to parent, subsidiary or affiliate entities within Acquia's corporate family, partner entities that are not within Acquia's corporate family and vendors and service agencies that we may engage to assist us in providing our services to you. For example, we may provide your personally identifiable information to a credit card processing company to process your payment. Such third party service providers may be obligated to protect your personally identifiable information consistent with the terms of this Privacy Policy and not for their promotional purposes and/or required to enter into written confidentiality and data processing agreements including the commitment to be compliant with the Standard Contractual Clauses issued by the European Commission. We will also disclose your personally identifiable information (a) if we are required to do so by law, regulation or other government authority, in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, or otherwise in cooperation with an ongoing investigation of a governmental authority (b) to enforce the Acquia Terms of Use agreement or to protect our rights or (c) to protect the safety of users of our Site and our services.

The Site may provide links to other Web sites or resources over which Acquia does not have control ("External Web Sites"). Such links do not constitute an endorsement by Acquia of those External Web Sites. You acknowledge that Acquia is providing these links to you only as a convenience, and further agree that Acquia is not responsible for the content of such External Web Sites. Your use of External Web Sites is subject to the terms of use and privacy policies located on the linked External Web Sites.

Security

We employ procedural and technological measures that are reasonably designed to help protect your personally identifiable information including sensitive data from loss, unauthorized access, disclosure, alteration or destruction. Acquia may use encryption, secure socket layer, firewall, password protection and other physical security measures to help prevent unauthorized access to your personally identifiable information including sensitive data. Acquia may also place internal restrictions on who in the company may access data to help prevent unauthorized access to your personally identifiable information. These precautions take into account the risks involved in the processing, the nature of personally identifiable information, and best practices in the industry for security and data protection.

Please find additional information about Acquia's security measures on our website https://www.acquia.com/solutions/security and for our Services specifically in our Acquia Security Annex available at https://www.acquia.com/sites/default/files/legal/acquia-security-annex.pdf

Accountability for Onward Transfer

Acquia is accountable for personally identifiable information that we receive and subsequently transfer to third parties. If third parties that process personally identifiable information on our behalf do so in a manner that does not comply with the Privacy Shield Principles, we are accountable, unless we prove that we are not responsible for the event giving rise to the damage.

Contact information and Customer personally identifiable information is accessible only by those Acquia employees and consultants who have a reasonable need to access such information in order for us to fulfill contractual, legal and professional obligations. All of our employees and consultants have entered into confidentiality agreements, and/or have been subjected to thorough criminal background checks requiring that they maintain the confidentiality of Customer personally identifiable information.

In the event Acquia discloses personally identifiable information covered by this Policy to a non-agent third party, it will do so consistent with any notice provided to Data Subjects and any choice they have exercised regarding such disclosure. Acquia will only disclose personally identifiable information to third-party agents that have given us contractual assurances that they will provide at least the same level of privacy protection as is required by this Privacy Policy and the Principles and that they will process personally identifiable information for limited and specific purposes consistent with any consent provided by the individual. If Acquia has knowledge that a third party to which it has disclosed personally identifiable information covered by this Privacy Policy is processing such personally identifiable information in a way that is contrary to this Privacy Policy and/or the Principles, Acquia will take reasonable steps to prevent or stop such processing. In such case, the third-party is liable for damages unless it is proven that Acquia is responsible for the event giving rise to the violation.

Acquia may use from time to time a limited number of third-party service providers, contractors, and other businesses to assist us in providing our solutions to our customers or in meeting internal business operation needs. These third-parties may access process or store personally identifiable information in the course of performing their duties to Acquia. Acquia maintains contracts with these providers restricting their access, use and disclosure of personally identifiable information in compliance with our obligations under the Principles.

YOUr rights relating to your personal data

Depending on the applicable local data protection laws, you have certain rights relating to your Personal Data including, but not limited to:

Access to your data

Rectification

Erasure ("right to be forgotten")

Restriction of Processing

Object, opt-out, withdrawing your consent

Transfer of your data

Acquia provides you with the ability to exert any such right by contacting us through this web form (https://acquia-privacy.my.onetrust.com/webform/29a25674-36fd-4a6f-8e09-7e5a4f94cf4a/8511aea7-dd1f-4353-9429-a0dbe52f01cc).

Enforcement and Liability

Acquia is subject to the jurisdiction and enforcement and investigatory authority of the United States Federal Trade Commission.

Acquia also commits to periodically reviewing and verifying the accuracy of this Policy and the company's compliance with the Principles, and remedying issues identified. All employees of Acquia that have access to personally identifiable information covered by this Policy in the U.S. are responsible for conducting themselves in accordance with this Policy. Failure of an Acquia employee to comply with this Policy may result in disciplinary action up to and including termination.

Acquia assures compliance with this EU-U.S. and Swiss-U.S. Privacy Shield Policy and the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks by utilizing the self-assessment approach as specified by the U.S. Department of Commerce. The assessment is conducted on an annual basis to ensure that all of Acquia's relevant privacy practices are being followed in conformance with this EU-U.S. and Swiss-U.S. Privacy Shield Policy and the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Any employee that Acquia determines is in violation of these policies will be subject to discipline, up to and including termination of employment and/or criminal prosecution.

Dispute Resolution

Acquia assures compliance with this EU-U.S. and Swiss-U.S. Privacy Shield Policy by fully investigating and attempting to resolve any complaint or dispute regarding the use and disclosure of personally identifiable information in violation of this Privacy Policy.

Any questions or concerns regarding the use or disclosure of personally identifiable information should first be directed to the owner of the website in question (our customer); or if the question or concern is from our customer, then to Acquia at the address given below.

Acquia will respond to any inquiries or complaints within forty-five (45) days. In the event that Acquia fails to respond or its response is insufficient or does not address the concern, Acquia has registered with JAMS to provide independent third party dispute resolution at no cost to the complaining party. To contact JAMS and/or learn more about the company's dispute resolution services, including instructions for submitting a complaint, please visit: https://www.jamsadr.com/eu-us-privacy-shield.

If your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

Acquia will cooperate with the United States Federal Trade Commissions and any data protection authorities of the EU Member States and/or United Kingdom ("DPAs") in the investigation and resolution of complaints that cannot be resolved between Acquia and the complainant that are brought to a relevant DPA.

Contact Us

If you have any questions or complaints regarding this Privacy Policy please contact us by mail: Acquia Inc. 53 State Street Boston, MA 02109 USA Attention: General Counsel

Or e-mail to privacy@acquia.com

Updated February 11, 2022

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 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 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.

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 disseminating, promoting or facilitating child pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming.

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.

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.

ACQUIA DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**DPA**"), which forms part of the Subscription and Services Agreement (the "Agreement") between Acquia and the customer specified on page 5 of this DPA ("**Customer**"), is entered into by Acquia and 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 pursuant to the Agreement, 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 the Agreement 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).

Except as modified below, the terms of the Agreement shall remain in full force and effect. Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. In case of a conflict between the terms of the DPA and the Agreement, the terms of the DPA shall prevail. This DPA supersedes and replaces all prior agreements between Customer and Acquia regarding the subject matter of this DPA.

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" as defined in the GDPR.

"**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.

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

"**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
- **[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 "personal data" as defined in the GDPR that is subjected to the Services under Customer's Agreement.

"**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").

"**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" as defined in the GDPR.

"**Product Notice**" means the "GDPR Product Notices" describing the Services privacy-relevant functions, features, and similar information as available under https://docs.acquia.com/guide/ .

"**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**"), as 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 Protection2018 – 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.

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 is the Data Controller and Acquia is the Data Processor with respect to 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.

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**. Effective from 25 May 2018, 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 extentAcquia 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.**

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 attached hereto as **Exhibit 2**, unless the Customer has opted out of those clauses.

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.

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).

10.3 **Data Production Request and Additional Safeguards.**

10.3.1 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:

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

10.3.3 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).

10.3.4 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.

10.3.5 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.

10.3.6 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.

11. 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.

12. 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)
Signature: _____	Signature: _____
Print Name:_____	Print Name: _____
Title: _____	Title: _____
E-mail: _____	
Date:	Date: _____

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:

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 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 principle of least privilege access, allowing only active Acquia employees and contractors access to records containing Customer Data and limits 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 Exhibit, 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 policies 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 the Security Annex apply. If, in the course of providing Subscription Services, Acquia agrees in writing to process such Customer Data andCustomer 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. In the event that 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 and the Agreement, and any amendments.

b. Acquia will comply with: (i) secure software development practices consistent with industry accepted standards and practices,and (ii) industry best practices on privacy and security.

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 to accomplish the intended business purpose or use. Acquia facilities and/or any Authroized Contractor facilities that process Customer Data will be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., electronic locks, access badges, and video surveillance) that provide a physically secure environment.

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

e. 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 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 assessAcquia'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 validateproper 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 Acquia Security Annex (the "Security Measures"). These Security Measures may be changed by Acquia from time to time during the Term of the Agreement in order to take into account advancements in available security technologies. However, Acquia will not materially decrease the overall security of the Services during the Term of the Agreement.

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 in order 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 andacknowledgment of professional behavior in the workplace documents, which includes anti-harassment and business 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

Pseudonymisation 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.

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 Customer Data 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. Subprocessors

Processes for evaluating prospective and existing Subprocessors 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, takes into account 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 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, regardingthe disposalof both tangible property and electronic files containing Customer Data, taking into account 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 inaccordance 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 applicable laws and regulations 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 SCCs, UK IDTA, Business Associate Agreement governing Protected Health Information), implementation of additional security controls required by relevant law, completion of regulatory filings applicable to Acquia, and participation inrelevant regulatory audits as applicable from section 13 below.

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 theServices, 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 filessufficient 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 facilitiesthat 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.

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's 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
Acquia Cloud Enterprise	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • HIPAA[1] • PCI-DSS[2] • FedRAMP[3]
Acquia Cloud Site Factory	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • HIPAA[1] • PCI-DSS[2] • FedRAMP[3]

[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 implementationis more fully described in its FedRAMP package, available via the OMB MAX repository system.

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 Customersupon 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:

a. Agreements with relevant subprocessors include requirements that these subprocessors address security risks, controls, and procedures for information systems and contain terms, conditions, and restrictions at least as protective and as restrictive asthose set forth herein. Acquia shall supply each of its personnel and contractors with appropriate, ongoing training regardinginformation 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 subprocessors for the Services and to support Acquia as a Processor of Customer data, all as more fully set forth on the website located at: https://www.acquia.com/about-us/legal/subprocessors. As these subprocessors are authorized subprocessors as defined in the Agreement,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 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 using AWS and a one-to-many business model that relies on standardization of best practices and industry standards for the benefit of its Customers. As a result, onsite audits by Customers pose security and privacy risks to Acquia, other Acquia Customers and Acquia Subprocessors. Moreover, AWS does not allow for physical audits of the AWS data centers but instead provides 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 "Third Party Audits, Certifications" 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 Subprocessors, 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 the section "Third Party Audits, Certification" 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)[1]

The Parties determine and agree that for purposes of this DPA, Module Two (Transfer controller to processor) applies. Clauses of other modules of the EU SCCs have been deleted for improved readability.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the EuropeanParliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([2]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 –Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 –Clause 9(a), (c), (d) and (e);

(iv) Clause 12 –Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 –Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

[1] For the types of Services provided by Acquia, as further stipulated in the DPA, the Customer is the Controller and Acquia the Processor of Personal Data. Thus, Module Two of these Clauses applies. Therefore, unless stipulated to the contrary in the DPA, Module Two of these Clauses [Controller-to-Processor relationship] applies.

[2] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another

processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws orpractices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due accountof the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature ofprocessing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub- processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([4]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importermay redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competentsupervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

[4] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(c) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(d) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(e) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(f) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, includingmeasures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles ofinternational comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competentsupervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on areasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter

may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliancewith these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to theprocessing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third- party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

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: per page 5 above

Address: per page 5 above

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 5 above

Role (controller/processor): 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, 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 5

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 therelevant 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: Autoriteit Persoonsgegevens of the Netherlands, 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"), 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, alsodescribe 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.

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 5 of this DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: per page 5 above Trading name (if different): per page 5 above Main address (if a company registered address): per page5 above Official registration number (if any) (company number or similar identifier): per page 5 above	Full legal name: Acquia Inc. Trading name (if different): n/a Main address (if a company registered address): 53State 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 5 above Reference (if any): Exhibit 2 of the DPA to which this Exhibit 3 is attachedOther 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 theExporter?
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")
3	n/a	n/a	n/a	n/a	n/a	n/a
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[6]

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.

[6] Alternative Part 2 Mandatory Clauses chosen.