ACQUIA DATA PROCESSING ADDENDUM[1]

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

This Data Processing Addendum (the "**DPA**") covers the Services (as further described below) provided by Acquia in, 53 State Street, 10th Floor, Boston, MA 02109, USA ("**Acquia**"), and any Acquia Affiliates, as applicable, that may Process Personal Data and which were sold either by Acquia directly or an authorized reseller ("**Reseller**") to the Customer specified on page 6 of this DPA ("**Customer**") under a respective end user services agreement or similar contract ("**Agreement**"). This DPA is entered into by Acquia and the Customer effective as of the last signature date below.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"**GDPR**" means

- **[European Union]** the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (also the "**EU GDPR**"),
- **[United Kingdom]** the "**UK GDPR**" (as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019), and
- **[Switzerland]** the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1;), and from 01 January 2023 onwards, the revised Swiss Federal Act on Data Protection of 25 September 2020 (both, as applicable, "**Swiss GDPR**").

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

[1] **How to execute this DPA:**

- This DPA has been pre-signed by Acquia (end of DPA main body on **page 6**).
- Complete any information required in
  - The signature boxes at the end of the DPA main body on **page 6**,
  - The information for the EU SCC Annexes I and II (**Exhibit 2** to this DPA)
  - The information for the UK IDTA **(Exhibit 3** to this DPA)
- Send the completed and signed DPA via email to privacy@acquia.com.
- Any additions, removals, or other modifications to the terms of this DPA (handwritten or otherwise) will render this DPA ineffective unless explicitly agreed to by Acquia separately in writing.

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

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

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

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

"**Standard Contractual Clauses**" means

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

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

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

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

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

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

1. DATA PROCESSING.

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

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

on behalf of and in accordance with Customer's documented instructions as set forth in Section 2.

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

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

2. CUSTOMER INSTRUCTIONS.

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

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

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

3. ACQUIA PERSONNEL.

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

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

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

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

4. TECHNICAL AND ORGANIZATIONAL MEASURES, CERTIFICATIONS, AUDITS.

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

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

5. SUB-PROCESSORS.

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

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

5.3 **Objection Right for new Sub-processors**. Customer may object to Acquia's use of a new Sub-processor by notifying Acquia promptly in writing within 10 business days after Acquia's update in accordance with the mechanism set out in Section 5.2 above. In the event Customer objects to a new Sub-processor: (i) Customer may immediately terminate the Agreement on giving written notice to Acquia; or (ii) where that objection is not unreasonable, Acquia will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid processing of Personal Data by the objected-to new Sub processor without unreasonably burdening Customer. If Acquia is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, without prejudice to Section 5.3 (i), Customer may terminate the applicable Order(s) in respect only to those Services which cannot be provided by Acquia without the use of the objected-to new Sub-processor, on the condition that Customer provides such termination notice within 90 days of being informed of the engagement of the Sub-processor as described in Section 5.2 above. If Customer terminates the Agreement under this Section 5.3, Acquia will then refund

Customer any prepaid fees covering the remainder of the term of such terminated Order(s) following the effective date of termination with respect of such terminated Services. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Sub-processor.

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

6. RIGHTS OF DATA SUBJECTS.

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

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

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION.

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

8. DATA PROTECTION IMPACT ASSESSMENT AND ASSISTANCE.

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

9. RETURN OR DELETION OF PERSONAL DATA.

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

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

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

10.2 **Standard Contractual Clauses.**

10.2.1 **Current Standard Contractual Clauses.**

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

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

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

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

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

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

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

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

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

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

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

11. DATA PRODUCTION REQUEST AND ADDITIONAL SAFEGUARDS.

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

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

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

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

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

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

12. CCPA/CPRA PROVISIONS

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

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

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

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

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

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

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

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

as such terms are defined in the CCPA/CPRA.

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

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

12.6 **Consumer Rights Requests**. Acquia shall notify Customer promptly if it receives a Consumer Rights Request concerning the processing of Personal Information and, in any event, in a reasonable amount of time for Customer to meet its obligations to respond to such Consumer Rights Request under the CCPA. Acquia shall not respond to any Consumer Rights Request concerning Personal Information unless

expressly instructed to do so by Customer, or otherwise required by law. To the extent Customer, in its use of the Services, does not have the ability to address a Consumer Rights Request, Acquia shall upon Customer's request assist Customer in responding to such Consumer Rights Request, to the extent Acquia is legally permitted to do so and the response to such Consumer Rights Request is required under the CCPA. To the extent legally permitted, Customer shall be responsible for any costs arising from Acquia's provision of such assistance.

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

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

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

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

Exhibit 1
to the ACQUIA GDPR DATA PROCESSING ADDENDUM
Security Annex

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

1. Security Policy.

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

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

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

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

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

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

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

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

2. Security Practices and Processes.

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

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

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

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

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

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

3. Patch and Vulnerability Management.

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

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

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

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

4. Security Monitoring.

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

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

5. Security of Data Processing.

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

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

a. Background Checks.

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

b. Training.

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

c. Customer Data.

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

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

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

d. Availability.

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

e. Logging and Monitoring.

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

f. Vulnerability Triaging.

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

g. Policies

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

h. Sub-processors.

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

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

6. Secure Data Transmissions.

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

7. Data and Media Disposal.

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

8. Backup and Retention.

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

9. Customer Data.

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

10. Security Incident Management and Remediation.

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

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

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

11. Business Continuity and Disaster Recovery.

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

12. Security Evaluations.

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

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

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

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

13. Acquia Certifications and Standards by Product Offering

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

Acquia Offering	**Completed Certifications and Attestations**

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

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

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

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

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

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

14. Training and Secure Development Practices.

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

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

15. Acquia Shared Responsibility Model.

Acquia Responsibilities

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

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

Customer Responsibilities

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

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

16. Access and Review.

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

17. Customer Audits.

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

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

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

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

ANNEX I

LIST OF PARTIES

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

1. Name: Customer per page 6 above and any Customer Affiliates as further described in the DPA and Agreement

Address: per page 6 above or as further described in the DPA and Agreement

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

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

Signature and date: per execution on page 6 above

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

2. _____

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

1. **Name**: Acquia Inc.

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

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

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

Signature and date: Per execution on page 6

Role (controller/processor): Processor.

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

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

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

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

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

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

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

Nature of the processing

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

Purpose(s) of the data transfer and further processing

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

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

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

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

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

COMPETENT SUPERVISORY AUTHORITY

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

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

ANNEX II

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

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

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

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

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

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

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

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

PART 1: TABLES

TABLE 1: PARTIES

Start date	from the date of last signature on page 6 of this DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: per page 6 above Trading name (if different): per page 6above Main address (if a company registered address): per page 6 above Official registration number (if any) (company number or similar identifier): per page 6 above	Full legal name: Acquia Inc. Trading name (if different): n/a Main address (if a company registered address): 53 State Street, Boston, MA 02109, USA Official registration number (if any) (company number or similar identifier): US Federal Tax ID (FEIN): 26-0493001
Key Contact	Full Name (optional): _____ Job Title: _____ Contact details including email: _____	Full Name (optional): n/a Job Title: Acquia Privacy Team Contact details including email: privacy@acquia.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: per page 6 above Reference (if any): Exhibit 2 of the DPA to which this Exhibit 3 is attached Other identifier (if any): n/a Or

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

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

Table 3: Appendix Information

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

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

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses[3]

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

[3] Alternative Part 2 Mandatory Clauses chosen.