ACQUIA GDPR 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 the last page ("**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.

"**Appendix**" herein means an appendix to the Standard Contractual Clauses; 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, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"**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; opposed to "Appendix" which means an appendix to the Standard Contractual Clauses.

"**GDPR**" means

- 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, and
- the UK GDPR (as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019).

"**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**" or "**SCCs**" means those standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as described in Article 46 of the GDPR and as adopted by the European Commission in decision 2010/87/EC dated 05 February 2010, as set forth in **Exhibit 1** hereto.

"**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 the GDPR or the 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 (https://www.acquia.com/about-us/legal/acquia-security-annex and also attached as **Exhibit 2**) 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 Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements.

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 SCCs.** Where Acquia processes Personal Data that originates from the European Union, the EEA, the United Kingdom and/or Switzerland, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the Standard Contractual Clauses in **Exhibit 1**, unless the Customer has opted out of those clauses.

10.2.2 **Follow-up SCCs.** 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 in the form set out in **Exhibit 1** 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 SCCs 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 Standard Contractual Clauses, 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.[1]

CUSTOMER:	ACQUIA INC.
Signature: _____	Signature: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
E-mail: _____	
Date:	Date: _____

[1] INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH ACQUIA:
For Acquia to execute this DPA, the above-named Customer must: (1) Have a current, in-force Subscription and Services Agreement with Acquia;* (2) Complete all the information in the signature bloc above and Have an authorized representative execute this DPA; (3) Send the completed and signed DPA to Acquia by email at DPA@acquia.com; (4) Acquia will countersign and return to the email address listed above, upon which this DPA shall come into effect and legally bind the parties.

* Please note that this DPA does not apply to on-line purchases of Acquia Cloud Platform Professional, which are covered by the ACPP Terms of Service.

Exhibit 1
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: _____

Address: _____

Tel. _____

Fax _____

E-mail: _____

Other information needed to identify the organisation

_____

(the **data exporter**)

And

Name of the data importing organisation: Acquia Inc.

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

Tel. +1 888 922 7842

e-mail: privacy@acquia.com

Other information needed to identify the organisation:

(the **data importer**)

each a '**party**'; together '**the parties**',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

CLAUSE 1
DEFINITIONS

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC[3];

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

CLAUSE 2
DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

CLAUSE 3
THIRD-PARTY BENEFICIARY CLAUSE

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

CLAUSE 4

[2] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

[3] References to Directive 95/46/EC in the Standard Contractual Clauses are treated as references to the relevant and respective clauses in the GDPR.

OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(c) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(d) that it will ensure compliance with the security measures;

(e) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(f) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(g) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(h) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(i) that it will ensure compliance with Clause 4(a) to (i).

CLAUSE 5

OBLIGATIONS OF THE DATA IMPORTER[4]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

[4] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

CLAUSE 6
LIABILITY

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

CLAUSE 7
MEDIATION AND JURISDICTION

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

CLAUSE 8
COOPERATION WITH SUPERVISORY AUTHORITIES

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

CLAUSE 9
GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

CLAUSE 10
VARIATION OF THE CONTRACT

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

CLAUSE 11
SUB-PROCESSING

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[5]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

CLAUSE 12
OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA-PROCESSING SERVICES

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

[5] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature .....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature .....

(stamp of organisation)

APPENDIX 1
TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

DATA EXPORTER: The data exporter is the Customer who subscribed to the Services as defined in the DPA and the Agreement.

DATA IMPORTER: The data importer is Acquia Inc., a provider of cloud platform related services, including PaaS and SaaS products, technical support services and professional consulting services for (Drupal) websites.

Acquia Affiliates support the Services remotely from the USA, India, the UK, and other locations where Acquia employs personnel in the delivery of the Services. Such support includes:

- Monitoring the Services for availability, performance, security, including intrusion detection and penetration testing
- Backup and restoration of Customer Data stored in the Services
- Development, updating, upgrading, and troubleshooting the Services and any underlying cloud infrastructure

DATA SUBJECTS:

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:
- representatives and end-users including employees, contractors, collaborators, customers, customer prospects, and advisors of data exporter (who are natural persons)

CATEGORIES OF DATA:

The personal data transferred concern the following categories of data (please specify):

- Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion. Customer can configure the data categories by designing and administering the Application, administering and configuring the Service itself, and in setting up specific Services (e.g. Acquia Edge CDN) that collect respective data from the visitors to Customer's Application.
- The Personal Data may include, but is not limited to the following categories of Personal Data:
    - First and last name
    - Title, work department, and manager/superviso 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

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE)

The personal data transferred concern the following special categories of data (please specify):

- The same concept applies as above under "Categories of data": Data exporter may submit special categories of data to the Services in accordance with the Agreement, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may – for the sake of clarity – include Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

PROCESSING OPERATIONS

The personal data transferred will be subject to the following basic processing activities (please specify):

- see the respective Product Notice in **Appendix 3**

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: .....

Authorised Signature .....

APPENDIX 2
TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL SECURITY MEASURES IMPLEMENTED BY THE DATA IMPORTER IN ACCORDANCE WITH CLAUSES 4(D) AND 5(C) (OR DOCUMENT/LEGISLATION ATTACHED):

- see the relevant Product Notice available online at https://docs.acquia.com/guide/ (marked as "GDPR Product Notice")
- see the Acquia Security Annex available online at https://www.acquia.com/sites/acquia.com/files/documents/2018-04/Acquia-Security-Annex.pdf and **Exhibit 2**

Exibit 2
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 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. 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 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 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 and acknowledgment 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 disposal of 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 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 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 Standard Contractual Clauses, 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 in relevant 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 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 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 implementation is 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.