

ACQUIA DATA PROCESSING ADDENDUM

This Data Processing Addendum (the “**DPA**”), which forms part of the Subscription and Services Agreement (the “**Agreement**”) between Acquia and the customer specified on page 5 of this DPA (“**Customer**”), is entered into by Acquia and Customer effective as of the last signature date below.

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

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

DEFINITIONS.

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

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

“**Acquia Affiliates**” means all Acquia Affiliates listed at <https://www.acquia.com/about-us/legal/subprocessors>.

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

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

“**Controller**” means “controller” as defined in the GDPR.

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

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

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

“**EEA**” means the European Economic Area.

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

“**GDPR**” means

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

“**Personal Data**” means “personal data” as defined in the GDPR that is subjected to the Services under Customer’s Agreement.

“**Product Notice**” means the respective notice describing privacy-related description of the Services, as available on Acquia’s website at <https://docs.acquia.com/guide/> (marked as “GDPR Product Notice”).

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

“**Processor**” means “processor” as defined in the GDPR.

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

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

“**Standard Contractual Clauses**” means

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

1. DATA PROCESSING.

1.1 **Scope and Roles.** This DPA applies when Personal Data is Processed by Acquia as part of Acquia’s provision of Services as agreed in the Agreement and the applicable Order. In this context, Customer is the Data Controller and Acquia is the Data Processor with respect to Personal Data.

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

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

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

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

2. CUSTOMER INSTRUCTIONS.

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

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

3. ACQUIA PERSONNEL.

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

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

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

3.4 **Data Protection Officer.** Effective from 25 May 2018, Acquia shall have appointed, or shall appoint, a data protection officer if Data Protection Laws require such appointment. Any such appointed person may be reached at privacy@acquia.com.

4. TECHNICAL AND ORGANIZATIONAL MEASURES, CERTIFICATIONS, AUDITS.

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

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

5. SUB-PROCESSORS.

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

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

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

5.4 **Acquia's Liability for Sub-processors.** Acquia shall be liable for the acts and omissions of its Sub-processors to the same 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.

Personal Data from the EU, EEA, Switzerland: Where Acquia processes Personal Data that originates from the European Union, the EEA, and/or Switzerland, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the EU SCCs as attached hereto as **Exhibit 2**, unless the Customer has opted out of those clauses.

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

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

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

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

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

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

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

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

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

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

11. **LIABILITY.**

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



12. TERM AND TERMINATION OF THE DPA.

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

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

CUSTOMER: _____
(data exporter)

ACQUIA INC.
(data importer)

Signature: _____

Signature: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____

E-mail: _____

Date: _____

Date: _____

Exhibit 1 to the ACQUIA GDPR DATA PROCESSING ADDENDUM Security Annex

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

1. Security Policy. Acquia maintains a company-wide information security management system and control program that includes written security policies, standards and procedures based upon ISO/IEC 27001:2013 (collectively, the “Acquia Information Security Policy”). The Acquia Information Security Policy requires:

- a. the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of Customer Data to the extent that such Customer Data is provided to Acquia and maintained or processed by Acquia during its provision of Services by utilizing practices such as:
 - i. Secure software development practices;
 - ii. Secure operating procedures and vulnerability management;
 - iii. Ongoing employee training;
 - iv. Controlling physical and electronic access to Customer Data, and
 - v. Means for detecting and preventing intrusions and security system failures on critical systems.
- b. that Acquia follow the principle of least privilege access, allowing only active Acquia employees and contractors access to records containing Customer Data and limits access to those persons who are reasonably required to know such information in order to accomplish a valid business purpose or to comply with record retention regulations;
- c. that Customer Data that is identified as such to Acquia by the customer at intake, is secured appropriately commensurate to the nature of Customer Data, including any individual personal data provided to Acquia by Customer as set forth in this Exhibit, using commercially available and industry accepted controls and precautionary measures;
- d. that commercially reasonable standards are followed with respect to strong change-control procedures and technical controls that enforce segregation of duties, minimum necessary dataset, and access controls;
- e. monitoring of operations and maintaining procedures to ensure that security policies are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Customer Data, and continuously improving information safeguards as necessary to mitigate risks;
- f. a security patch and vulnerability management process based on accepted industry standard practices and protocols, including, monitoring threats, and responding to vulnerabilities reported by third parties; and
- g. A security incident response and disaster recovery planning, including documentation of responsive actions taken in connection with any security incident related to Customer Data.

2. Security Practices and Processes

- a. Customers are responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any Customer Data processed, stored or transmitted through the Subscription Services for which regulations other than those set forth in the Security Annex apply. If, in the course of providing Subscription Services, Acquia agrees in writing to process such Customer Data 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 Authorized 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, regarding the 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 SCCs, UK IDTA, Business Associate Agreement governing Protected Health Information), implementation of additional security controls required by relevant law, completion of regulatory filings applicable to Acquia, and participation 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 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.

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	<ul style="list-style-type: none"> ● SOC 1 Type 2 (SSAE18 & ISAE 3402) ● SOC 2 Type 2 (Security, Availability and Confidentiality) ● ISO 27001:2013 ● HIPAA¹ ● PCI-DSS² ● FedRAMP³
Acquia Cloud Site Factory	<ul style="list-style-type: none"> ● SOC 1 Type 2 (SSAE18 & ISAE 3402) ● SOC 2 Type 2 (Security, Availability and Confidentiality) ● ISO 27001:2013 ● HIPAA¹ ● PCI-DSS² ● FedRAMP³

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

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 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:

- 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 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 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 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

Exhibit 2 EU SCCs (Standard Contractual Clauses 2021)¹

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

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

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

² Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

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

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent

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

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ⁽⁴⁾ The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation,

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

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

- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards⁵;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

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

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of the Netherlands.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

LIST OF PARTIES

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

1. Name: per page 5 above

Address: per page 5 above

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

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

Signature and date: per execution on page 5 above

Role (controller/processor): Controller

2. _____

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

1. Name: Acquia Inc.

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

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

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

Signature and date: Per execution on page 5

Role (controller/processor): Processor.

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

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

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

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

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

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

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

Nature of the processing

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

Purpose(s) of the data transfer and further processing

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

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

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

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

As specified in the relevant Product Notice per each Service available at <https://docs.acquia.com/guide/> in connection with 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: Autoriteit Persoonsgegevens of the Netherlands, and

Where the Swiss GDPR applies: Federal Data Protection and Information Commissioner of Switzerland

ANNEX II

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

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

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

For transfers to (sub-) processors, 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.

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

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

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

PART 1: TABLES

Table 1: Parties

Start date	from the date of last signature on page 5 of this DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	<p>Full legal name: per page 5 above</p> <p>Trading name (if different): per page 5 above</p> <p>Main address (if a company registered address): per page 5 above</p> <p>Official registration number (if any) (company number or similar identifier): per page 5 above</p>	<p>Full legal name: Acquia Inc.</p> <p>Trading name (if different): n/a</p> <p>Main address (if a company registered address): 53 State Street, Boston, MA 02109, USA</p> <p>Official registration number (if any) (company number or similar identifier): US Federal Tax ID (FEIN): 26-0493001</p>
Key Contact	<p>Full Name (optional):</p> <p>_____</p> <p>Job Title:</p> <p>_____</p> <p>Contact details including email:</p> <p>_____</p>	<p>Full Name (optional): n/a</p> <p>Job Title: Acquia Privacy Team</p> <p>Contact details including email: privacy@acquia.com</p>
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p><input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: per page 5 above</p> <p>Reference (if any): Exhibit 2 of the DPA to which this Exhibit 3 is attached</p> <p>Other identifier (if any): n/a</p> <p>Or</p> <p><input type="checkbox"/> 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:</p>
------------------	--

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”)
3	n/a	n/a	n/a	n/a	n/a	n/a
4	n/a	n/a	n/a	n/a	n/a	n/a

Table 3: Appendix Information

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

Annex 1A: List of Parties:

Exhibit 2 Annex I to the DPA

Annex 1B: Description of Transfer:

Exhibit 2 Annex I to the DPA

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Exhibit 2 Annex II to the DPA

Annex III: List of Sub processors (Modules 2 and 3 only):

<https://www.acquia.com/about-us/legal/subprocessors>

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p><input checked="" type="checkbox"/> Importer</p> <p><input checked="" type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
---	--

Mandatory Clauses

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

⁶ Alternative Part 2 Mandatory Clauses chosen.