DATA PROCESSING ADDENDUM

Last Updated April 14, 2026

This Data Processing Addendum ("**DPA**") forms part of the applicable subscription and services agreement (the "**Agreement**"), entered by and between the Customer named in the Agreement and PerformanceCentre, Inc. ("**Performio**"), pursuant to which Customer has purchased subscriptions to Performio's application services ("**Services**"). By entering into the Agreement that references or incorporates this DPA, Customer agrees to be bound by the terms of this DPA. The purpose of this DPA is to reflect the parties' agreement about the Processing of Personal Data, in accordance with the requirements of Applicable Data Protection Laws.

If the Customer entity subject to this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

If the Customer entity subject to this DPA has entered an Order Form with Performio pursuant to the Agreement (an "**Ordering Document**"), but is not itself a party to the Agreement, this DPA is an addendum to that Ordering Document and applicable renewal Ordering Documents. Each Customer Affiliate that enters into its own Ordering Document under the terms of the Customer's Agreement shall likewise be entitled to the rights and obligations of this DPA, provided, however, each Customer Affiliate shall exercise its rights under this DPA through Customer, unless otherwise required by applicable law.

This DPA will be effective and will replace and supersede any previously applicable terms relating to their subject matter (including any data Processing amendment, agreement or addendum relating to the Services), from the effective date of the Agreement or, if later, the date this DPA is first made available at the URL referenced above ("DPA Effective Date").

DATA PROCESSING TERMS

For the duration of the Agreement and in the course of providing the Services to Customer pursuant to the Agreement, Performio may Process Personal Data on behalf of Customer. This DPA applies where Performio processes Personal Data as a Processor (or Sub-Processor as applicable) on behalf of Customer and such Personal Data is subject to Applicable Data Protection Laws (as defined below).

The parties have agreed to enter this DPA to provide appropriate safeguards for such Personal Data in accordance with Applicable Data Protection Laws. Accordingly, Performio agrees to comply with the following provisions with respect to any Personal Data that it processes as a Processor (or Sub-Processor as applicable) on behalf of Customer.

1. DEFINITIONS. Capitalized terms will have the meanings set forth below unless defined elsewhere in this DPA or the Agreement.

"**Adequate Country**" means a country or territory that is recognized under European Data Protection Laws as providing adequate protection for Personal Data.

"**Affiliate**" means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists).

"**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including without limitation European Data Protection Laws, the CCPA/CPRA, and any other applicable national, federal, state, or provincial data protection or privacy law.

"**CCPA/CPRA**" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 - 1798.199), as amended by the California Privacy Rights Act of 2020 and any regulations issued pursuant thereto.

"**Controller**" means an entity that determines the purposes and means of the Processing of Personal Data and shall have the meanings given to them in GDPR, and for the purposes of this DPA, includes equivalent terms used under other Applicable Data Protection Laws.

"**Customer Data**" shall have the meanings given to it in the Agreement.

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

"**Data Subject**" means the individual to whom Personal Data relates

"**European Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and the United Kingdom applicable to the Processing of Personal Data under the Agreement (including, where applicable, (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "EU GDPR"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii)).

"**European Economic Area**" or "**EEA**" means the European Economic Area, namely the European Union Member State along with Iceland, Liechtenstein and Norway.

"**GDPR**" means General Data Protection Regulation 2016/679 and UK GDPR from 31.12.2020;

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

"**Personal Data**" means any information relating to an identified or identifiable natural person, or that is otherwise defined as "personal data," "personal information," "personally identifiable information," or any analogous term under Applicable Data Protection Laws.

"**Processor**" means the entity that Processes Personal Data on behalf of the Controller and shall have the meanings given to them in GDPR, and for the purposes of this DPA, includes equivalent terms used under other Applicable Data Protection Laws

"**Processing**" shall have the meanings given to them in GDPR

"**Regulator**" means any Supervisory Authority or regulatory body with responsibility for ensuring compliance with Data Protection Laws and Regulations.

"**Restricted Transfer**" means: (i) where the EU GDPR or Swiss Federal Act on Data Protection applies, a transfer of Personal Data from the European Economic Area or Switzerland (as applicable) to a country outside of the European Economic Area or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and Information Commissioner (as applicable); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Services**" shall refer to the cloud-based solutions offered, marketed or sold by Performio and shall have the meanings given to them in the Agreement.

"**SCCs**" or "**Standard Contractual Clauses**" means the standard contractual clauses as adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Sub-Processor**" means any third-party Processor engaged by Performio to Process Personal Data in order to provide the Services to Customer under the Agreement and/or this DPA.

"**Supervisory Authority**" means an independent public authority which is established by a member state pursuant to Article 51 of the GDPR or, for the United Kingdom, the Information Commissioner's Office ("**ICO**").

"Swiss Addendum" means the standard data protection clauses for the transfer of Personal Data to third countries pursuant to the Swiss Federal Act on Data Protection (FADP) and its revised version (revFADP) in force 1 September 2023, as issued by the Swiss Federal Data Protection and Information Commissioner (FDPIC), supplementing the Standard Contractual Clauses to the extent required to comply with Swiss data protection law.

"UK Addendum" means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0 in force 21 March 2022, in line with S119A(1) UK Data Protection Act 2018.

All other capitalized definitions in this DPA not explicitly defined in this DPA, shall have the same meanings as defined in the Agreement, the GDPR or other Applicable Data Protection Laws , in that order of precedence.

2. STATUS OF THE PARTIES

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the Processing and the categories of Data Subjects, are as described in Schedule 1.

2.2 Each party warrants in relation to Personal Data that it will comply with Applicable Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties acknowledge and agree that the Customer is the Controller (or a Processor Processing Personal Data on behalf of a third-party Controller), and Performio is a Processor (or Sub-processor, as applicable).

2.4 If Customer is a Processor, Customer warrants to Performio that Customer's instructions and actions with respect to the Personal Data, including its appointment of Performio as another Processor and, where applicable, concluding the SCCs, have been (and will, for the duration of this DPA, continue to be) authorized by the relevant third-party Controller.

3. PROCESSING OF PERSONAL DATA

3.1 Roles of the Parties. The parties acknowledge and agree that regarding the Processing of Personal Data, Customer is the Controller and determines the purposes for which and the manner in which the Personal Data is Processed, Performio is the Processor of any Personal Data, acting on behalf of the Customer. Performio may engage Sub-Processors pursuant to the requirements set forth in Section 7 "Sub-Processors" below. Each party, in respect of the Processing of the Personal Data acknowledges and agrees that each party has respective rights and obligations under Applicable Data Protection Laws.

3.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws. For the avoidance of doubt, Customer will ensure that its instructions for the Processing of Personal Data comply with Applicable Data Protection Laws. Customer will ensure that Performio's Processing of Personal Data, when done in accordance with the Customer's instructions, will not cause Performio to violate any applicable law or regulation, including Applicable 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. Customer shall ensure that the Customer is entitled to transfer the relevant Personal Data to Performio so that Performio and its Sub-Processors may lawfully use, process and transfer the Personal Data in accordance with this DPA and the Agreement on Customer's and its Affiliates' behalf. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under Applicable Data Protection Laws. Performio will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate any applicable law or regulation, including Applicable Data Protection Laws.

3.3 Performio's Processing of Personal Data. Performio shall Process Personal Data on behalf of and in accordance with Customer's written instructions and shall treat Personal Data as Confidential Information, provided that any exclusions or carve-outs that apply to Confidential Information under the Agreement shall not apply to Personal Data. Customer instructs Performio to Process Personal Data for the following purposes:

(i) Processing in accordance with the Agreement and applicable Ordering Document, which includes updating the Services and preventing or addressing service or technical issues;

(ii) Processing initiated by Customer's Authorized Users in their use of the Services;

(iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement and Applicable Data Protection Laws; and

(iv) as otherwise required by applicable law. The Agreement and this DPA, along with Customer's configuration and use of the Services, are Customer's complete and final instructions to Performio in relation to the Processing of Personal Data, including for purposes of the Standard Contractual Clauses, and any Processing required outside of the scope of these

instructions (inclusive of the rights and obligations set forth under the Agreement) will require prior written agreement of the parties.

3.4 Data Residency. With respect to the Services, Performio may store data in Australia or the United States. Personal Data received through the Services may be disclosed to, transferred to, and/or allowed to be accessed by or otherwise Processed by Performio's personnel or Sub-Processors. Personal Data may be transferred to personnel of Performio and/or its Affiliates located in the European Union and other European countries, the United Kingdom, Australia, Canada, the United States and India in the course of the Services. Any intragroup transfer is subject to an intragroup data Processing agreement. Performio will notify Customer if the foregoing list of countries changes (which notice may be provided through communication channels, Performio's website, or such other reasonable means). In the event that a new country is added to the foregoing list of countries to which Personal Data may be transferred, the parties agree to cooperate in good faith in meeting any additional regulatory or legal requirements necessary to allow such transfers. Notwithstanding the foregoing, with the exception of Personal Data processed through the Services, certain Personal Data may be stored by Performio or its Sub-Processors in the U.S. for operational purposes.

4. RIGHTS OF DATA SUBJECTS

Taking into account the nature of the Processing and the information available to Performio, Performio assists the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Applicable Data Protection Laws. Performio shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment, or deletion of that person's Personal Data. Performio shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. To the extent Customer, in its use of the Services, does not have the ability to access, correct, amend, block, or delete Personal Data as required by Applicable Data Protection Laws, Performio shall provide Customer with commercially reasonable cooperation and assistance in responding to such request, to the extent Performio is legally permitted to do so.

5. PERFORMIO OBLIGATIONS:

With respect to all Personal Data it processes in its role as a Processor or Sub-processor, Performio warrants that it shall:

(i) only process Personal Data in order to provide the Service and in accordance with: (i) the Customer's written instructions as set out in the Agreement and this DPA, unless required to do so by applicable Union or Member State law to which Performio is subject, and (ii) the requirements of Applicable Data Protection Laws. In the event Performio is required to process Personal Data under Applicable Data Protection Laws, Performio shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Performio shall promptly inform Customer if Performio determines that it can no longer meet its obligations under this DPA or under Applicable Data Protection Laws;

(ii) not sell, retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Service, including for a commercial purpose other than providing the Service. Performio shall not use the Personal Data for the purposes of marketing or advertising. Performio shall not Share (as defined under the CCPA/CPRA or any similar term used in other Applicable Data Protection Laws) Personal Data for cross-context behavioral advertising. Performio's performance of the Service may include disclosing Personal Data to Sub-Processors where this is in accordance with Section 7 of this DPA;

(iii) inform Customer if, in Performio's opinion, any instructions provided by the Customer under Section 3.3 infringe Applicable Data Protection Laws;

(iv) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the Processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Schedule 2 ("Security Measures"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Performio may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Service;

(v) ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under contractual or statutory obligations of confidentiality;

(vi) without undue delay notify the Customer upon becoming aware of any breach of security leading to the accidental

or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed for the purpose of providing the Services to Customer by Performio, its Sub-processors, or any other identified or unidentified third party (a "Personal Data Breach") and provide the Customer with reasonable cooperation and assistance in respect of that Personal Data Breach, including all reasonable information in Performio's possession concerning such Personal Data Breach insofar as it affects the Personal Data;

(vii) not make any public announcement about a Personal Data Breach (a "Breach Notice") without the prior written consent of the Customer, unless required by applicable law;

(viii) promptly notify Customer if Performio receives a request from a Data Subject to exercise any data protection rights (including rights of access, rectification or erasure) in respect of that Data Subject's Personal Data (a "Data Subject Request"). Performio shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees;

(ix) to the extent Performio is able, and in line with applicable law, provide reasonable assistance to Customer in responding to a Data Subject request to exercise any data protection rights (including rights of access, rectification or erasure) in respect of that Data Subject's Personal Data if the Customer does not have the ability to address a Data Subject Request without Performio's assistance. The Customer is responsible for verifying that the requestor is the Data Subject in respect of whose Personal Data the request is made. Performio bears no responsibility for information provided in good faith to Customer in reliance on this subsection. Customer shall cover all costs incurred by Performio in connection with its provision of such assistance;

(x) other than to the extent required to comply with applicable law, following termination or expiry of the Agreement or completion of the Service, at the choice of Customer, delete or return all Personal Data (including copies thereof) processed pursuant to this DPA;

(xi) to the extent Performio is able to verify that a Data Subject is associated with the Customer, promptly notify the Customer if it receives a request from a Data Subject to exercise any Data Subject right, taking into account the nature of Processing and the information available to Performio;

(xii) provide such assistance to the Customer as the Customer reasonably requests in relation to Performio's obligations under Applicable Data Protection Laws with respect to:

(a) data protection impact assessments and prior consultations (as such terms are defined in Applicable Data Protection Laws);

(b) notifications to the supervisory authority under Applicable Data Protection Laws and/or communications to Data Subjects by the Customer in response to any Personal Data Breach; and

(c) the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to the security of Processing.

6. PERFORMIO PERSONNEL

6.1 Confidentiality. Performio shall ensure that its personnel and those of its Affiliates engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

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

7. SUB-PROCESSORS

7.1 Appointment of Sub-Processors. Customer acknowledges and agrees that Performio's Affiliates may be retained as Sub-Processors, and Performio and Performio's Affiliates respectively may engage third-party Sub-Processors in connection with the provision of the Services, in each case:

(i) anywhere in the world where Performio, its Affiliates or its or their Sub-Processors maintain data Processing operations; and

(ii) subject to a written agreement requiring the Sub-Processor to comply with the requirements of Applicable Data Protection Laws and to abide by terms no less protective of the Customer Personal Data than those provided in this DPA to the extent applicable to the nature of the services provided by such Sub-Processor.

7.2 Performance by Sub-Processor. Performio shall be liable for any such Sub-Processor's performance of any obligation under this DPA.

7.3 Current Sub-Processors. Performio shall not sub-contract its Processing of Personal Data, or otherwise permit any third party to process Personal Data, without Customer's prior general authorization, which is hereby granted for the Processing of Personal Data by (i) Sub-Processors authorized to provide services under the Agreement in order to perform such services, and (ii) Sub-Processors to the extent necessary, while providing ancillary administrative, infrastructure and other support services to Performio. Performio's Sub-Processors approved by Customer as a condition to entering into this DPA are listed at https://www.performio.co/legal-documents.

7.4 Requirements of Sub-Processors. Performio shall not disclose, transfer and/or grant access to Personal Data to a Sub-Processor unless Performio: (a) executes a written agreement with such Sub-Processor that contains substantially similar data protection obligations imposed on Performio by this DPA, including implementing appropriate technical and organizational measures; and (b) remains liable for the Sub-Processor's failure to fulfil its obligations with respect to the Processing of Personal Data as if Performio had failed to fulfill such obligations.

7.5 Objections. Performio will provide at least thirty (30) days advance written notice of any new Sub-Processor. If Customer has a reasonable basis to object to Performio's use of a new Sub-Processor, Customer shall notify Performio in writing within ten (10) business days. In the event Customer objects to a new Sub- Processor(s) on reasonable grounds, and Performio chooses to retain the objected-to new Sub-Processor, Performio will notify the Customer in writing. Within ten (10) business days of such notification, Customer may provide written notice to terminate those Services in the applicable Ordering Document(s) in respect only to those Services which cannot be provided by Performio and/or a mutually agreed upon Sub-Processor without the use of the objected-to new Sub- Processor. Within thirty (30) days of receipt of such notice from Customer, Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

8. SECURITY

8.1 Controls for the Protection of Personal Data. Performio shall maintain appropriate administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data that are appropriate to (a) the size, scope and type of Performio's business; (b) the amount of resources available to Performio; (c) the type of information that Performio will store; and (d) the need for security and confidentiality of such information. Performio shall regularly monitor compliance with these safeguards. At a minimum, Performio will implement and maintain the technical and organizational measures set forth in Schedule 2. Performio reserves the right to update such measures provided that any updates shall not materially diminish the level of security applicable to the Services during a Subscription Term.

8.2 Audits.

(a) At least once per year during the term of the Agreement, Performio shall have an audit of its operations performed by an independent auditing firm. This audit will include an evaluation that tests and validates key controls relating to the security of Personal Data (currently a SSAE 18 SOC 2 report) ("**Audit Report").**

(b) Performio shall, in accordance with Applicable Data Protection Laws, make available to Customer such Audit Report with a view to demonstrating Performio's compliance with the obligations of Processors under Applicable Data Protection Laws in relation to its Processing of Personal Data. Subject to the confidentiality provisions of the Agreement, Performio shall make a summary of the then-current Audit Report available to Customer. The Customer agrees that any audit rights granted by Applicable Data Protection Laws will be satisfied by these Audit Reports.

(c) The Audit Report shall fulfil Customer's right of audit under Applicable Data Protection Laws in relation to Personal Data, provided that (a) the Audit Report is not older than thirteen (13) months, prepared by an independent external auditor demonstrating that Performio's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard; (b) that additional information in Performio's possession or control shall be provided to a data protection supervisory authority when it requests or requires additional information in relation to the Processing of Personal Data carried out by Performio under this DPA; and (c) to the extent that Customer's Personal Data is subject to SCCs and the information made available pursuant to this Section 8.2 is insufficient, in Customer's reasonable judgment, to confirm Performio's compliance with its obligations under this DPA or Applicable Data Protection Laws, then Performio shall enable Customer to request one onsite audit per annual period during the Term (as defined in the Agreement) to verify Performio's compliance with its obligations under this DPA in accordance with Section 8.2

(d) The following additional terms shall apply to audits the Customer requests:

i. Customer must send any requests for reviews of Performio's Audit Reports to legal@performio.co.

ii. provides notice to Performio in a timely fashion;
iii. requests access only during business hours;
iv. occurs no more than once annually;
v. restricts its finding to only data relevant to Customer; and
vi. obligates Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

(e) Performio may charge a fee (based on Performio's reasonable costs) for any onsite audit under this Section 8.2. Performio will provide Customer with further details of any applicable fee and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(f) Following receipt by Performio of a request for audit under this Section 8.2, Performio and Customer will discuss and agree in advance on the reasonable start date, scope, duration of, and security and confidentiality controls applicable to any audit under this Section 8.2. Whenever possible, evidence for such an audit will be limited to the evidence collected for Performio's most recent third-party audit.

(g) Performio may object in writing to an auditor appointed by Customer to conduct any audit under this Section 8.2 if the auditor is, in Performio's reasonable opinion, not suitably qualified or independent, a competitor of Performio, or otherwise manifestly unsuitable (i.e., an auditor whose engagement may have a harmful impact on Performio's business comparable to the aforementioned aspects). Any such objection by Performio will require Customer to appoint another auditor or conduct the audit itself. If the SCCs apply, nothing in this Section 8.2 varies or modifies the SCCs nor affects any supervisory authority's or Data Subject's rights under the SCCs.

8.3 Data Protection Impact Assessment and Prior Consultation. Performio shall provide reasonable assistance to Customer with any data protection impact assessments (at Customer's expense only if such reasonable cooperation will require Performio to assign significant resources to that effort) and prior consultations with any Supervisory Authority or other competent data privacy authorities to the extent required by Applicable Data Protection Laws, in each case solely in relation to Processing of Personal Data, and taking into account the nature of the Processing and information available to Performio.

9. DATA TRANSFERS FROM THE EEA, SWITZERLAND, AND THE UK

9.1 Location of Processing. In connection with the Service, the parties anticipate that Performio (and its Sub-processors) may process outside of the European Economic Area ("EEA"), Switzerland, and the United Kingdom, certain Personal Data protected by European Data Protection Laws in respect of which Customer, or a member of the Customer Group may be a Controller (or Processor on behalf of a third-party Controller, as applicable).

9.2 Transfer mechanisms. The transfer of Personal Data subject to this DPA may only occur in accordance with data transfer mechanisms as permitted or required by Applicable Data Protection Laws, including but not limited to:

(a) Standard Contractual Clauses ("SCCs") as further specified in Schedule 3;
(b) Adequacy decisions or equivalent determinations issues by relevant Regulators; or
(c) Model contracts or any other applicable data transfer mechanism recognized by relevant Regulators.

9.3 Restricted Transfers. The parties agree that when the transfer of Personal Data protected by European Data Protection Laws from Customer or any member of the Customer Group to Performio is a Restricted Transfer then it shall be subject to Schedule 3.

9.4 Onward Restricted Transfers. In respect of Restricted Transfers made to Performio under Section 9.3, Performio shall not participate in (nor permit any Sub-processor to participate in) any further Restricted Transfers of Personal Data (whether as a "Data Exporter" or an "Data Importer" of the Personal Data) unless such further Restricted Transfer is made in full compliance with European Data Protection Laws and pursuant to SCCs implemented between the Data Exporter and Data Importer of the Personal Data or an Alternative Transfer Mechanism (as defined in Section 9) adopted by the Data Importer applies.

9.5 Assessments. In the event Customer seeks to conduct any assessment of the adequacy of the SCCs for transfers to any particular countries or regions, Performio shall, to the extent it is able, provide reasonable assistance to Customer for the purpose of any such assessment, provided Customer shall cover all costs incurred by Performio in connection with its provision of such assistance.

9.6 Alternative mechanisms. To the extent Performio adopts an alternative data export mechanism (including the EU-US. Data Privacy Framework or any successor thereto adopted pursuant to applicable European Data Protection Laws) for the transfer of Personal Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Laws and extends to the territories to which Personal Data is transferred), and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to such Alternative Transfer Mechanism. In the event that an applicable transfer mechanism is invalidated and Performio is unable to provide an alternative lawful transfer mechanism within a reasonable period, Customer may terminate the affected Services upon written notice and shall receive a pro-rated refund of any prepaid fees for the period following the effective date of termination.

10. THIRD PARTY DATA ACCESS REQUESTS

10.1 If Performio becomes aware of any third-party legal process requesting Personal Data that Performio processes on behalf of Customer in its role as Processor or Sub-Processor (as applicable) then Performio will:

(a) immediately notify Customer of the request unless such notification is legally prohibited;

(b) inform the third party that it is a Processor or Sub-processor (as applicable) of the Personal Data and is not authorized to disclose the Personal Data without Customer's consent;

(c) disclose to the third party the minimum necessary Customer contact details to allow the third party to contact the Customer and instruct the third party to direct its data request to Customer; and

(d) to the extent Performio provides access to or discloses Personal Data in response to third party legal process either with Customer authorization or due to a mandatory legal compulsion, then Performio will disclose the minimum amount of Personal Data to the extent it is legally required to do so and in accordance with the applicable legal process.

10.2 In Performio's role as a Processor or Sub-processor, as applicable, it may be subject to third party legal process issued by a government authority (including a judicial authority) and requesting access to or disclosure of Personal Data. If Performio becomes aware of any third party legal process issued by a government authority (including a judicial authority) requesting Personal Data that Performio processes on behalf of Customer in its role as Processor or sub- Processor (as applicable) then, to the extent that Performio reviews the request with reasonable efforts and as a result is able to identify that such third party legal process requesting Personal Data raises a conflict of law, Performio will:

(i) take all actions identified in Section 10.1 above;

(ii) pursue legal remedies prior to producing Personal Data up to an appellate court level; and

(iii) not disclose Personal Data until (and then only to the extent) required to do so under applicable procedural rules.

10.3 Sections 10.1 and 10.2 shall not apply in the event that Performio has a good-faith belief the government request is necessary due to an emergency involving the danger of death or serious physical injury to an individual. In such event, Performio shall notify Customer of the data disclosure as soon as possible following the disclosure and provide Customer with full details of the same, unless such disclosure is legally prohibited.

11. SECURITY BREACH MANAGEMENT AND NOTIFICATION

Performio maintains security incident management policies and procedures and shall, to the extent permitted by law, notify Customer's designated contact as set forth by Customer in the signature block below, without undue delay (and in any event within 48 hours of confirmation), of any breach of security leading to the actual or reasonably suspected unauthorized disclosure of Personal Data by Performio or its Sub-Processors of which Performio becomes aware (a "**Security Breach**"). For the avoidance of doubt, "Security Breach" does not include pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing, or similar incidents. Any such notification is not an acknowledgement of fault or responsibility. To the extent such Security Breach is caused by a violation of the requirements of this DPA by Performio, Performio shall make reasonable efforts to identify and remediate the cause of such Security Breach. Performio will reasonably assist the Customer to comply with its reporting obligations under Applicable Data Protection Laws in connection with the Security Breach, including by providing at least the following information to the extent available:

(a) a description of the nature of the Security Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) a description of the likely consequences of the Security Breach;
(d) a description of the measures taken or proposed to be taken to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In case of a Security Breach and prior to making any required public statement or required notice, Customer agrees to timely provide Performio with a draft for discussion on the content of its intended required public statements or required notices for the affected Data Subjects and/or required notices to the relevant Regulators regarding the Security Breach to the extent such public statements or notices identify Performio by name or relate to Performio's multi-tenant cloud software and/or Services. This draft shall be discussed in a timely fashion and in good faith between the parties. Notwithstanding the preceding sentence, Customer shall not be required to prejudice its obligations under Applicable Data Protection Laws.

12. RETURN AND DELETION OF PERSONAL DATA

12.1 Performio shall make Personal Data available for export by Customer upon written request made within thirty (30) days of the date of termination/expiration of the Agreement. Unless prohibited by applicable law, within sixty (60) days after the termination/expiration of the Agreement, Performio shall securely destroy all Personal Data in its possession or control. Upon Customer's written request, Performio shall provide written certification that all Personal Data has been securely destroyed.

12.2 Notwithstanding anything to the contrary in this Section 12, Performio may retain Personal Data, if required by applicable law or regulation or in furtherance of the Agreement, including Applicable Data Protection Laws or for electronic backups, provided such Personal Data remains protected in accordance with the terms of the Agreement, this DPA and Applicable Data Protection Laws.

13. INTERNATIONAL PROVISIONS

13.1 Conditions for International Processing. Performio shall be entitled to Process Personal Data, including by using Sub-Processors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Laws and Regulations.

13.2 Jurisdiction Specific Terms. To the extent Performio Processes Personal Data originating from and protected by Data Protection Laws and Regulations in one of the jurisdictions listed in Schedule 4 "Jurisdiction Specific Terms" of this DPA, the terms specified in Schedule 4 with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

13.3 International Data Transfer Mechanisms for Data Transfers. To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer Personal Data from a jurisdiction (i.e., the EEA, the United Kingdom, Switzerland, or any other jurisdiction listed in Schedule 4) to Performio located outside of that jurisdiction ("**Transfer Mechanism**"), the terms set forth in Schedule 3 "International Transfer Mechanisms" will apply.

13.4 Conflict. In the event of any conflict or inconsistency among the following documents, the conflict or inconsistency shall be resolved by giving precedence in the following order: (i) the applicable terms of Schedule 4 "Jurisdiction Specific Terms"; (ii) the Standard Contractual Clauses as applicable; and (iii) this DPA.

14. GENERAL

14.1 This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail to the extent the subject matter concerns the Processing of Personal Data.

14.2 Performio's liability under or in connection with this DPA, including under the SCCs, is subject to the exclusions and limitations on liability contained in the Agreement. In no event does Performio limit or exclude its liability towards Data Subjects or competent data protection authorities.

14.3 Except where and to the extent expressly provided in the SCCs or required as a matter of Applicable Data Protection Laws, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

14.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws as specified in the

Agreement, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts specified in the Agreement.

14.5 If any provision of this DPA is, for any reason, held to be invalid or unenforceable, the other provisions of the DPA will remain enforceable. Without limiting the generality of the foregoing, Customer agrees that Section 14.2 (Limitation of Liability) will remain in effect notwithstanding the unenforceability of any provision of this DPA.

14.6 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Performio may update this DPA from time to time by posting a revised version at the URL where this DPA is made available. Updates will become effective upon posting; provided that any update that materially diminishes Customer's rights or materially increases Customer's obligations under this DPA will not apply during an existing Subscription Term unless required to comply with applicable law or Customer agrees otherwise.

Schedule 1 - Description of the Processing

1. DATA SUBJECTS

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Customer's employees, agents, advisors, and contractors who are natural persons, and Customer's users authorized by Customer to use the Services.

2. CATEGORIES OF PERSONAL DATA

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

Names and contact details, e-mail and telephone details, job title, unit/department, employee identification number, employment status and type, compensation information, including bonus and sales commission eligibility, quotas, commission rates and on target earnings, objectives, coaching and job performance information.

3. SPECIAL CATEGORY DATA

None.

4. FREQUENCY OF PROCESSING

Continuous.

5. PURPOSES OF THE TRANSFER / PROCESSING OPERATIONS

The objective of Processing of Personal Data by Performio is the performance of the Services pursuant to the Agreement. Performio shall only Process Personal Data in accordance with the instructions as set out by Section 3.3 of the DPA.

6. PERIOD FOR WHICH THE PERSONAL DATA WILL BE RETAINED

See section 12 of this DPA.

Schedule 2 - Technical and Organizational Security Measures

Where applicable, this Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of Annex II to the 2021 Standard Contractual Clauses (2021) and Applicable Data Protection Laws.

Performio will implement and maintain the technical and organizational measures as set forth in Performio's SOC 1 Type II and SOC 2 Type II audit report. Performio reserves the right to update such measures at its sole discretion provided that any updates shall not materially diminish the level of security applicable to the Services during an existing Subscription Term.

The technical and organizational measures implemented by Performio (including any relevant certifications) to ensure an appropriate level of security, considering the nature, scope, context, and purposes of the processing, and the risks to the rights and freedoms of natural persons, are as follows:

Encryption of personal data

- Data at rest encrypted using, at a minimum, AES-256 algorithm or compensating controls are in place (including hashed passwords and encrypted machines).
- Employee laptops are encrypted using full disk AES-256 encryption.
- HTTPS encryption on every web login interface, using industry standard algorithms and certificates.
- Secure transmission of credentials using by default TLS 1.2.
- Access to operational environments requires the use of secure protocols such as HTTPS.
- Data resides in Amazon Web Services (AWS) encrypted at rest, as stated in AWS' documentation and whitepapers.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Strong access controls use the principle of least privilege.
- Differentiated rights system based on security groups and access control lists.
- Employees are granted only the access necessary to perform their job functions.
- Unique accounts and role-based access within operational and corporate environments.
- Access to systems is restricted by security groups and access-control lists.
- Authorization requests are tracked, logged, and audited on a regular basis.
- Employee access is removed upon termination or change of employment.
- Enforcement of Multi-factor Authentication (MFA) for access to critical and production resources.
- Strong and complex passwords are required. Initial passwords must be changed after the first login.
- Passwords are never stored in clear text and are encrypted in transit and at rest.
- Account provisioning and de-provisioning processes.
- Segregation of responsibilities and duties to reduce opportunities for unauthorized or unintentional modification or misuse.
- Confidentiality requirements are imposed on employees.
- Mandatory security training for employees, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and overall security responsibilities inside and outside of Performio.
- Nondisclosure agreements with third parties.
- Separation of networks based on trust levels.

Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing

- User activity, including logins, configuration changes, deletions, and updates, are written automatically to audit logs in operational systems.
- All logs can be accessed only by authorized Performio employees, and access controls are in place to prevent unauthorized access.
- Write access to logging data is strictly prohibited. Logging facilities and log information are protected against tampering and unauthorized access using access controls and security measures.
- Network segmentation and interconnections are protected by AWS Security Groups that are reviewed at least bi-annually to ensure all configurations are appropriate.
- Regular vulnerability scans are performed on externally accessible systems.
- Performio employs automated system patching services to ensure production infrastructure is patched timely.

Measures for user identification and authorization

- Access to operational and production environments is protected using unique user accounts, strong passwords, Multi-Factor Authentication (MFA), role-based access, and the least privilege principle.
- Authorization requests and provisioning are logged, tracked, and audited.
- User activity in operational environments, including access, modification, or deletion of data, is being logged.
- A Web Application Firewall (WAF), in addition to network-based security controls, is in place.

Measures for the protection of Data during transmission

- HTTPS encryption for data in transit (using TLS 1.2 or greater).

Measures for the protection of Data during storage

- Performio customer instances are logically separated using dedicated database schemas.
- Logins and data access are logged and monitored.
- Endpoint security software is deployed to all Performio managed systems.
- System inputs recorded via log files.
- Access Control Lists (ACL) are in place.
- Multi-factor Authentication (MFA) is in place.

Measures for ensuring system configuration, including default configuration

- Performio has formal Third Party Risk Management Procedures in place that include change management.
- Performio monitors changes to in-scope systems to confirm that changes follow the process, and to mitigate the risk of undetected changes to production.
- Performio has in place access control policy and procedures.

Measures for ensuring data minimization

- Data collection is limited to the purposes of the processing.
- Security measures are in place to provide only the minimum amount of access necessary to perform required functions.

Measures for ensuring limited data retention

- After termination of all subscriptions associated with an environment, customer data submitted to the Services is retained in inactive status within the Services until deleted in accordance with Performio's data retention processes.

Schedule 3 – International Data Transfer Mechanisms

The purpose of this Schedule 3 is to ensure the protection of natural persons with regard to the Processing of their Personal Data in light of data transfers of such Personal Data between countries with varying levels of privacy and data protection.

1. THE PARTIES

Each Party to this Schedule 3 is as follows:

Data Exporter(s):

The Data Exporter is the Customer (as defined in this DPA) and its Affiliates (as defined in the Agreement) established in the EEA, the UK or Switzerland that have purchased Services pursuant to one or more Ordering Documents.

Contact details of the Data Exporter are as set forth in the Agreement or applicable Ordering Document.

Data Exporter role: Controller or Processor (as applicable)

Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed the SCCs, UK Addendum and Swiss Addendum, where applicable, including their Annexes, as of the Effective Date of the Agreement.

Data Importer(s):

The Data Importer is Performio, a provider of hosted incentive compensation, performance management and territory optimization software applications, which processes Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

Contact details: Performio Legal Team – legal@performio.co

Data Importer Role: Processor.

Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed the SCCs, UK Addendum and Swiss Addendum, where applicable, including their Annexes, as of the Effective Date of the Agreement.

2. APPLICABLE DATA TRANSFER REQUIREMENTS

2.1 To the extent Personal Data originates in the EEA and is transferred to a country for which the European Commission has not granted an EU Adequacy Decision, the Parties shall comply with the Standard Contractual Clauses and applicable supplementary measures, to the extent required. The Standard Contractual Clauses are hereby incorporated by reference into, and form an integral part of, this DPA, and shall apply as follows:

a) The Standard Contractual Clauses shall be governed by Module Two where the Data Exporter is a Controller and the Data Importer a Processor.

b) The Standard Contractual Clauses shall be governed by Module Three where the Data Exporter is a Processor and the Data Importer a Processor (or Sub-Processor).

c) For the purposes of Clause 7 (Docking clause) of the Standard Contractual Clauses, the Parties agree that the optional docking clause shall not apply to the Parties.

d) For the purposes of Clause 9(a) (Use of Sub-Processors) of the Standard Contractual Clauses, the Parties agree that 'Option 2' is incorporated therein and shall apply to the Parties, whereby a time period of 30 (thirty) days is specified.

e) For purposes of Clause 11 (Redress) of the Standard Contractual Clauses, the Parties agree that the optional wording is not incorporated therein and does not apply to the Parties.

f) For purposes of Clause 13 (Supervision) and Annex I.C of the Standard Contractual Clauses, the Parties agree that the competent supervisory authority shall be the Dutch supervisory authority ('Autoriteit Persoonsgegevens').

g) For purposes of Clause 17 (Governing law) of the Standard Contractual Clauses, the Parties agree that 'Option 1' is incorporated therein and shall apply to the Parties, meaning the Standard Contractual Clauses shall be governed by the law of the Netherlands.

h) For purposes of Clause 18(b) (Choice of forum and jurisdiction) of the Standard Contractual Clauses, the Parties agree that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the Netherlands.

i) For purposes of Annex I of the Appendix to the Standard Contractual Clauses (Description of transfer), the Parties agree that Schedule 1 applies.

j) For purposes of Annex II of the Appendix to the Standard Contractual Clauses, the Parties agree that the technical and organisational security measures set forth in Schedule 2 apply and shall be implemented and maintained.

k) The Parties acknowledge that Annex III of the Appendix to the Standard Contractual Clauses does not apply.

l) The Parties agree not to transfer Personal Data outside the EEA, except to the extent such transfer is i) in accordance with the Standard Contractual Clauses or ii) Parties have an independent legal basis to facilitate such a transfer.

2.2 To the extent Personal Data originates in the UK and is transferred to a country for which the UK authorities have not granted or recognised an adequacy status, the Parties agree to be bound by the terms and conditions set out in the UK Addendum. The UK Addendum is hereby incorporated by reference into and forms an integral part of this Schedule 3, and shall apply as follows:

a) For purposes of Table 1 under Part 1 of the UK Addendum, the Start Date is the signing date of the Standard Contractual Clauses.

b) For purposes of Table 1 under Part 1 of the UK Addendum, the Parties' Details are provided under clause 1 of this Schedule 3.

c) For purposes of Table 1 under Part 1 of the UK Addendum, the Key Contact information of both the Data Exporter(s) and the Data Importer(s) is provided under clause 1 of this Schedule 3.

d) For purposes of Table 2 under Part 1 of the UK Addendum, the Parties select the Standard Contractual Clauses as agreed to by the Parties by function of this Schedule 3.

e) For purposes of Table 3 under Part 1 of the UK Addendum, the Appendix Information regarding the List of Parties is provided under clause 1 of this Schedule 3.

f) For purposes of Table 3 under Part 1 of the UK Addendum, the Appendix Information regarding the Description of Transfer is provided under Schedule 1.

g) For purposes of Table 3 under Part 1 of the UK Addendum, the Appendix Information regarding the Technical and Organisational Measures is provided in Schedule 2.

h) For purposes of Table 4 under Part 1 of the UK Addendum, the Parties agree that any Data Exporter or Data Importer may end the UK Addendum in line with Section 19 thereof.

2.3 To the extent Personal Data originates in Switzerland and is transferred to a country for which the Swiss authorities have not granted or recognised an adequacy status, the Parties agree to be bound by the terms and conditions set out in the SCCs, supplemented and amended by the Swiss Addendum, which is hereby incorporated by reference.

2.4 To the extent there is any conflict between the SCCs, UK Addendum or Swiss Addendum and any other terms in this DPA, including Schedule 4 (Jurisdiction Specific Terms) of this DPA, the Agreement, the provisions of the SCCs, UK Addendum or Swiss Addendum will prevail.

Schedule 4 – Jurisdiction Specific Terms

1. AUSTRALIA

1.1 The definition of "Applicable Data Protection Laws" includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Laws.

2. UNITED STATES

2.1 The definition of "Applicable Data Protection Laws" includes the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 *et seq.*) as may be amended from time to time including CCPA/CPRA and all other applicable US state data privacy and data protection laws, as amended from time to time (collectively with the CCPA/CPRA, "**US Privacy Laws**").

2.2 The definition of "Personal Data" includes "Personal Information," "Personal Data," or analogous terms as defined under US Privacy Laws.

2.3 The definition of "Data Subject" includes "Consumer," "Resident," or analogous terms as defined under US Privacy Laws. Any Data Subject rights, as described in Section 4 "Rights of Data Subjects" of this DPA, apply to consumer or resident rights under US Privacy Laws. In regard to Data Subject requests, Performio can only verify a request from Customer and not from any third party.

2.4 The definition of "Controller" includes "Business," "Controller," or analogous terms as defined under US Privacy Laws.

2.5 The definition of "Processor" includes "Service Provider," "Processor," or analogous terms as defined under US Privacy Laws.

2.6 To the extent the Personal Data Processing activities are subject to US Privacy Laws, Performio will comply with the obligations set forth in this Section 2.6. Performio will not retain, use, sell or otherwise disclose Personal Data:
(a) for any purposes other than as set forth in the Agreement and this DPA, unless otherwise required by law, or (b) outside of the direct business relationship between Customer and Performio, except as permitted under applicable Data Protection Laws and Regulations. Performio certifies that it understands these restrictions and obligations and will comply with them. For purposes of this Section 2.6, the terms "sell," "share," and analogous terms have the meanings given in the applicable US Privacy Laws.

2.7 Performio certifies that its Sub-Processors, as described in Section 7 "Sub-Processors" of this DPA, are Service Providers or Processors (as applicable) under US Privacy Laws, with whom Performio has entered into a written contract that includes terms substantially similar to this DPA. Performio conducts appropriate due diligence on its Sub-Processors. Performio will implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Data it processes as set forth in Section 8 "Security" and Schedule 2 of this DPA.

2.8 Performio shall not Share Personal Data for cross-context behavioral advertising or targeted advertising purposes. For purposes of this Section, "Share" and "targeted advertising" have the meanings given in the applicable US Privacy Laws.

2.9 To the extent any US state enacts or amends data privacy or data protection legislation that imposes obligations on Performio as a Processor, service provider, or analogous role, Performio shall comply with such obligations to the extent applicable to its Processing of Personal Data under the Agreement, and the terms of this Section 2 shall be interpreted to give effect to such obligations.

3. CANADA

3.1. The definition of "Applicable Data Protection Laws" includes the Federal Personal Information Protection and Electronic

Documents Act (PIPEDA).

3.2. Performio's Sub-Processors, as described in Section 7 "Sub-Processors" of this DPA, are third parties under PIPEDA, with whom Performio has entered into a written contract that includes terms substantially similar to this DPA. Performio has conducted appropriate due diligence on its Sub-Processors.

3.3. Performio will implement technical and organizational measures as set forth in Section 8 "Security" and Schedule 2 of this DPA.
3.4. Performio will implement technical and organizational measures as set forth in Section 8 "Security" and Schedule 2 of this DPA.

4. EUROPEAN ECONOMIC AREA (EEA)

4.1 The definition of "Applicable Data Protection Laws" includes the General Data Protection Regulation (EU 2016/679) on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data ("GDPR").

4.2 When Performio engages a Sub-Processor under Section 7 "Sub-Processors" of this DPA, it will: (a) require any appointed Sub-Processor to protect the Personal Data to the standard required by GDPR, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR, and (b) require any appointed Sub-Processor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the Standard Contractual Clauses (2021) or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

4.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

5. ISRAEL

5.1 The definition of "Applicable Data Protection Laws" includes the Protection of Privacy Law (PPL).

5.2 The definition of "Controller" includes "Database Owner" as defined under PPL.

5.3 The definition of "Processor" includes "Holder" as defined under PPL.

5.4 Performio will require that any personnel authorized to process Personal Data comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Laws. Such personnel sign confidentiality agreements with Performio in accordance with Section 6.1 "Confidentiality" of this DPA.

5.5 Performio must take sufficient steps to ensure the privacy of Data Subjects by implementing and maintaining the security measures as specified in Section 8 "Security" and Schedule 2 of this DPA and complying with the terms of the Agreement.

5.6 Performio must ensure that the Personal Data will not be transferred to a Sub-Processor unless such Sub-Processor has executed an agreement with Performio pursuant to Section 7 "Sub-Processors" of this DPA.

6. JAPAN

6.1. The definition of "Applicable Data Protection Laws" includes the Act on the Protection of Personal Information (APPI).

6.2. The definition of "Personal Data" includes "Personal Information" as defined under the APPI.

6.3. The definition of "Controller" includes "Business Operator" as defined under APPI. As a Business Operator, Performio is responsible for the handling of Personal Data in its possession.

6.4. The definition of "Processor" includes a business operator entrusted by the Business Operator with the handling of Personal Data in whole or in part (also a "trustee"), as described under APPI. As a trustee, Performio will ensure that the use of the

entrusted Personal Data is securely controlled.

7. SWITZERLAND

7.1. The definition of "Applicable Data Protection Laws" includes the Swiss Federal Act on Data Protection.

7.2. When Performio engages a Sub-Processor under Section 7 "Sub-Processors" of this DPA, it will: (a) require any appointed Sub-Processor to protect the Personal Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR, and (b) require any appointed Sub-Processor to
(i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

8. UNITED KINGDOM (UK)

8.1. References in this DPA to GDPR will, to that extent, be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

8.2. When Performio engages a Sub-Processor under Section 7 "Sub-Processors" of this DPA, it will: (a) require any appointed Sub-Processor to protect the Personal Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR; and (b) require any appointed Sub-Processor to
(i) agree in writing to only process Personal Data in a country that the United Kingdom has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

8.3. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.