PerformYard, Inc.

Data Protection Addendum

This Data Protection Addendum, including its Appendix ("**DPA**") forms part of the Master Subscription Agreement ("**Principal Agreement**") between PerformYard, Inc. acting on its own behalf and as agent for each of its Affiliates (collectively, "**Vendor**"), and **Customer** acting on its own behalf and as agent for each of its Affiliates.

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Principal Agreement. Except where the context requires otherwise, references in this DPA to the Principal Agreement are to the Principal Agreement as amended by, and including, this DPA.

How to Execute this DPA: This DPA has been pre-signed on behalf of PerformYard, Inc. To complete this DPA, Customer must (i) complete the information in the signature box and sign where indicated, and (ii) send the signed DPA to operations@performyard.com.

1. **Definitions**

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer or Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.2 "**Applicable Data Protection Laws**" means all national, federal, state, provincial, or local privacy, cybersecurity, and data protection laws, together with any implementing or supplemental rules and regulations, applicable to the Processing of Customer Personal Data under this DPA, as amended or replaced from time to time;

1.1.3 "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020;

1.1.4 "**Customer**" means the entity that executed the Principal Agreement together with its Affiliates;

1.1.5 "**Customer Personal Data**" means any Personal Data Processed by Vendor on behalf of Customer pursuant to or in connection with the Principal Agreement;

1.1.6 "**Data Privacy Framework**" means, collectively, the EU-US data privacy framework developed by the U.S. Department of Commerce and the European Commission, the UK Government's UK-US data bridge, and the Swiss Federal Administration's Swiss-US data privacy framework, all designed to provide U.S. organizations with reliable mechanisms to lawfully transfer personal data to the United States from the European Union, United Kingdom, and Switzerland.

1.1.7 "**GDPR**" means 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);

1.1.8 "**Member State**" means a member state of the European Economic Area ("EEA");

1.1.9 "**Restricted Transfer**" means a transfer or an onward transfer of Customer Personal Data, where such transfer would be prohibited by Applicable Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of an adequacy decision, a permitted derogation, a transfer framework, or other protection for the transferred Customer Personal Data provided by the SCCs, or other mechanism specified under Applicable Data Protection Law;

1.1.10 "**Security Incident**" means (i) any Personal Data Breach affecting Customer Personal Data, or (ii) any other event resulting in the unauthorized or unlawful access to, use, disclosure, loss, alteration or destruction of Customer Personal Data;

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Customer pursuant to the Principal Agreement;

1.1.12 "**Standard Contractual Clauses**" or "**SCCs**" means, as applicable to the relevant data transfer: (i) Module 2 of the standard contractual clauses set out in the Commission Implementing Decision (EU) 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 ("**Module 2 SCC**"), (ii) the UK IDTA, or (iii) such other terms intended to provide adequate protection to transferred personal data pursuant to Data Protection Law; in each case, as amended or replaced from time to time under the relevant Data Protection Law;

1.1.13 "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of Customer in connection with the Principal Agreement;

1.1.14 "**Third Country**" means: (i) with respect to GDPR, a country other than the Member States; (ii) with respect to the UK Data Protection Law, any country outside of the UK; and (iii) with respect to any other country, as provided in relevant Data Protection Law ;

1.1.15 "**UK Data Protection Law**" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended), and other Data Protection Laws in force from time to time in the United Kingdom; and

1.1.16 "**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, as amended or

replaced from time to time by a competent authority under the relevant Data Protection Laws.

1.2 The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing,**" "**Processor**," and "**Supervisory Authority**" and analogous terms shall have the same meaning as in Applicable Data Protection Laws (or where not defined in Applicable Data Protection Laws, shall have the meaning as in the GDPR), and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. **Authority**

Vendor warrants and represents that, before any Vendor Affiliate Processes any Customer Personal Data on behalf of any Customer Group Member, Vendor's entry into this DPA as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

3. **Processing of Customer Personal Data**

3.1 Vendor shall:

3.1.1 comply with Applicable Data Protection Laws in the Processing of Customer Personal Data; and

3.1.2 not Process Customer Personal Data other than on the Customer's documented instructions unless Processing is required by applicable law, in which case Vendor shall, to the extent permitted by applicable law, inform Customer of that legal requirement before Processing that Customer Personal Data.

3.2 Customer:

3.2.1 instructs Vendor (and authorises Vendor to instruct each Subprocessor) to:

3.2.1.1 Process Customer Personal Data; and

3.2.1.2 as needed, transfer Customer Personal Data to Third Countries,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement;

3.2.2 agrees that the Principal Agreement (including these DPA Terms and any applicable updates), along with Customer's use and configuration of the Services, are Customer's complete documented instructions to Vendor for the processing of Customer Personal Data; and

3.2.3 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each of its Affiliates.

3.3 Annex 1 to this DPA sets out certain details regarding Vendor's Processing of Customer Personal Data. Nothing in Annex 1 confers any right or imposes any obligation on any party to this DPA.

4. **Vendor Personnel**

Vendor shall grant access to Customer Personal Data on a need-to-know basis, as necessary for the purposes of the Principal Agreement and to comply with applicable laws, and shall ensure that all individuals authorized to Process Customer Personal Data are appropriately trained and subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. **Security**

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor shall implement the technical and organizational measures specified in Annex 2 to ensure an appropriate level of security for Customer Personal Data; and, further, if, at any time, a Supervisory Authority mandates specific additional measures, the Parties shall work together in good faith to implement such measures.

6. CCPA Terms

6.1 To the extent that Vendor Processes any Customer Personal Data subject to the CCPA, Vendor agrees to the following solely with regards to such Customer Personal Data:

6.1.1 All Customer Personal Data disclosed by Customer to Vendor, or that Vendor receives or processes on Customer's behalf, is disclosed or received only for limited and specified purposes, including for one or more business or commercial purposes as those terms are defined under the CCPA.

6.1.2 Vendor shall not sell, share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Customer Personal Data received from, or on behalf of, Customer to any third party for monetary or other valuable consideration.

6.1.3 Vendor shall not retain, use, or disclose Customer Personal Data received from, or on behalf of, Customer: (i) for any purposes (including, but not limited to, any commercial purpose) other than a business purposes specified in the Principal Agreement, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Vendor.

6.1.4 Vendor shall not combine Personal Data that it receives from, or on behalf of, Customer with Personal Data that Vendor receives from, or on behalf of, another person, or collects from its own interaction with an individual, unless the combining of that Personal Data is expressly permitted by the CCPA or regulations issued by the California Privacy Protection Agency. For purposes of this DPA, "combine" means to aggregate personal information about an individual into a single profile.

6.1.5 If Customer provides Vendor with deidentified Customer Personal Data, or if Vendor deidentifies Customer Personal Data, Vendor agrees to take reasonable measures to ensure that the deidentified Customer Personal Data cannot be associated with a consumer or household, and not attempt to reidentify the personal information.

6.1.6 If Vendor makes a determination it can no longer meet its obligations under the CCPA, it shall promptly notify Customer of this fact.

6.1.7 Vendor certifies it understands the obligations and restrictions above and will comply with them.

7. **Subprocessing**

7.1 Customer hereby grants Vendor general written authorisation to appoint (and permit each Subprocessor to appoint) Subprocessors in accordance with this section 6. Vendor's current list of Subprocessors engaged in Processing of Customer Personal Data can be found https://performyard.com/sub-processors, and Customer consents to Vendor's use of such Subprocessors.

7.2 The Subprocessor list page accessible via the link above contains a mechanism to subscribe to notifications of new Subprocessors. Vendor shall provide Customer thirty (30) days' notice prior to engaging any new Subprocessor using the subscription mechanism. Should Customer notify Vendor in writing to PerformYard, Inc., 4201 Wilson Blvd #110420, Arlington, VA 22203 USA of its reasonable objection to the proposed Subprocessor within thirty (30) days of receiving notice, the parties shall negotiate in good faith to find a suitable alternative Subprocessor. If no agreement is reached between the parties, Customer shall have the right to terminate the portion of the Principal Agreement as it relates to the use of the objected-to Subprocessor by Vendor.

7.3 With respect to each Subprocessor, Vendor shall:

7.3.1 include terms in the agreement between Vendor and Subprocessor that provides for, in substance, the same data protection obligations as those binding on Vendor under this DPA;

7.3.2 remain fully liable to Customer for any act or omission of its Subprocessor;

7.3.3 if that arrangement involves a Restricted Transfer, ensure that the relevant SCCs or transfer mechanism is, at all relevant times, entered into between Vendor and the Subprocessor; and

7.3.4 provide to Customer for review such copies of the agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Customer may request from time to time.

7.4 Where Vendor engages a Vendor Affiliate as a Subprocessor, such Vendor Affiliate may engage further Subprocessors subject to all the above terms and conditions.

8. **Data Subject Rights**

8.1 Taking into account the nature of the Processing, the functionality of the Services, and Vendor's role as a Processor, Vendor shall provide mechanisms or reasonable support to Customer to enable Customer to respond to requests by Data Subjects to exercise rights under Applicable Data Protection Laws ("**Data Subject Requests**").

8.2 Vendor shall:

8.2.1 promptly notify Customer if it receives a Data Subject Request; and

8.2.2 not respond to a Data Subject Request except on the documented instructions of Customer or as required by Applicable Data Protection Laws, in which case

Vendor shall, to the extent permitted, inform Customer of that legal requirement before the Contracted Processor responds.

9. **Personal Data Breach**

9.1 Vendor shall notify Customer without undue delay, but after a reasonable period to allow Vendor to investigate and, if necessary, involve law enforcement, upon Vendor becoming aware of an actual Security Incident. Vendor shall provide Customer with sufficient information to allow Customer to assess and meet its obligations to report a Security Incident under Applicable Data Protection Laws, which may be provided in stages as it becomes available to Vendor.

9.2 Vendor shall co-operate with Customer and take such commercially reasonable steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Security Incident.

10. **Data Protection Impact Assessment and Prior Consultation**

Vendor shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, as may be required by Applicable Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, Vendor.

11. **Deletion or return of Customer Personal Data**

11.1 Subject to sections 11.2 and 11.3, Vendor shall promptly and in any event within sixty (60) days of the date of termination of the Principal Agreement (the "**Cessation Date**"), delete and procure the deletion of Customer Personal Data.

11.2 Subject to section 11.3, Customer may, by written notice to Vendor within thirty (30) days of the Cessation Date and at Customer's expense, request Vendor return a complete copy of all Customer Personal Data to Customer by secure file transfer in such format as is reasonably notified by Customer to Vendor.

11.3 Vendor may retain Customer Personal Data to the extent and for such period as may be required by applicable laws. Vendor shall continue to protect all such Customer Personal Data and only Process such Customer Personal Data as necessary for the purpose(s) specified in the applicable laws.

11.4 Upon Customer's request, Vendor shall provide written certification to Customer that Vendor has complied with its requirements under this section 11.

12. **Audit rights**

12.1 Customer acknowledges that (i) Vendor's infrastructure is entirely cloud-based, and (ii) Vendor is regularly audited against industry security standards by independent third-party auditors, including obtaining an annual SOC 2 Type II audit report. Upon request, Vendor shall supply Customer a summary of its most recent SOC 2 Type II audit report(s), which reports shall be subject to the confidentiality provisions contained in the Principal Agreement. Pursuant to Applicable Data Protection Law, Customer, or its independent third-party auditor, may audit Vendor's security practices only if:

12.1.1 Vendor has been unable to provide sufficient evidence of its compliance with its obligations under this DPA or Applicable Data Protection Law by providing

summaries or copies of its independent audit reports, the sufficiency of which shall be based on a reasonable assessment by Customer;

12.1.2 An audit is formally requested by a Supervisory Authority; or

12.1.3 Applicable Data Protection Law confers on Customer such a right, provided that Customer shall not conduct such an audit more than once in any 12-month period, unless applicable Data Protection Law requires otherwise.

12.2 The rights set out in clause 12.1 will be exercised in accordance with the following principles:

12.2.1 any audit will be exercised taking a risk-based approach, considering the context and the nature of the Services, and adhering to relevant, commonly accepted audit standards;

12.2.2 if Customer appoints a third-party to exercise its audit rights, Customer will use commercially reasonable efforts to verify that (i) the auditor is not a competitor of Vendor, and (ii) the third-party auditor's personnel have acquired the right skills and knowledge to perform effective and relevant audits and assessments of the Services;

12.2.3 Customer acknowledges that all of Vendor's information technology infrastructure is cloud-based (hosted by Vendor's Subprocessors), and all staff work remotely, and therefore on-site audits are not possible;

12.2.4 audits will be restricted to Vendor's normal business hours, and will not interfere with Vendor's business operations; and

12.2.5 if the exercise of any audit right could, in Vendor's reasonable opinion, create a risk for another Vendor customer's environment, Customer and Vendor may agree on an alternative way to address the request to provide a similar level of assurance.

12.3 If an audit under this Section 12 results in a determination that Vendor has not established reasonable and adequate security controls for compliance with Vendor's obligations under this DPA, such a finding shall not constitute a breach of the DPA or the Principal Agreement provided Vendor remedies the deficiency within thirty (30) business days.

13. **Restricted Transfers**

13.1 Where Vendor has certified its adherence to the Data Privacy Framework and has been and is currently approved by the U.S. Department of Commerce as a participating member of the Data Privacy Framework, the parties shall rely on the Data Privacy Framework for Restricted Transfers to the United States to the extent (a) the Customer Personal Data is covered under the scope of Vendor's certification and approval, and (b) Vendor is and continues to be an active participating member of the Data Privacy Framework, as approved and recognized by the U.S. Department of Commerce. Notwithstanding the foregoing, the Standard Contractual Clauses shall take effect with respect to such Restricted Transfers immediately (or to the extent the parties have not entered into the Standard Contractual Clauses, the Parties shall enter into the Standard Contractual Clauses promptly) upon the occurrence of any of the following:

13.1.1 The Data Privacy Framework is invalidated, overturned, or revoked; or

13.1.2 Vendor's certification and/or approval to the Data Privacy Framework lapses, is withdrawn, is revoked, or is otherwise invalidated.

13.2 Vendor understands that Customer may be required to disclose privacy and security related terms of the Agreement, including this DPA, to the U.S. Department of Commerce or other regulators to meet its own obligations under applicable laws, and Vendor agrees that Customer may disclose a summary or a representative copy of the relevant privacy and security provisions of the Agreement upon such regulator's request.

13.3 Should the Standard Contractual Clauses apply to any Restricted Transfer, Customer (as "data exporter") and Vendor (as "data importer"), with effect from the commencement of the relevant Restricted Transfer, hereby enter into: (i) the Module 2 SCCs, which are expressly incorporated by reference herein, in respect of any Restricted Transfer subject to GDPR (subject to Section 13.2); and (ii) the UK IDTA, which is expressly incorporated by reference herein, in respect of any Restricted Transfer subject to UK Data Protection Law (subject to Section 13.3). Further, until such time as the relevant jurisdiction(s) issue their own standard contractual clauses, the Module 2 SCCs shall apply in respect of any Restricted Transfer subject to any other Data Protection Law that regulates cross-border transfers of Personal Data.

13.4 The parties agree that with respect to the Module 2 SCC:

13.4.1 *Clause 7 - Docking clause* shall not apply;

13.4.2 In *Clause 9 - Use of subprocessors*, Option 2 shall apply and the "time period" shall be thirty (30) days;

13.4.3 In *Clause 11(a) - Redress*, the optional language shall not apply;

13.4.4 In *Clause 13(a) - Supervision*, the following shall be inserted: 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 1.C, shall act as competent supervisory authority.

13.4.5 In *Clause 17 - Governing law*, Option 2 shall apply and the "Member State" shall be Ireland;

13.4.6 In *Clause 18 - Choice of forum and jurisdiction*, the Member State shall be Ireland;

13.4.7 Annex I shall be deemed completed with the relevant sections of Annex 1 to this DPA.

13.4.8 Annex II shall be deemed completed with the relevant sections of Annex 2 to this DPA; and

13.4.9 Annex III shall be deemed completed with the relevant sections of Annex 3 to this DPA.

13.5 In respect of Restricted Transfers from the UK, the SCCs (as incorporated by reference) shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA, and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is as set forth below:

13.5.1 Table 1 - the Parties are Vendor and Customer, with contact details as set forth in Annex 1 to this DPA.

13.5.2 Table 2 - the Approved EU Standard Contractual Clauses with optional provisions as set forth in Section 13.2.

13.5.3 Table 3 - the Annexes are deemed completed with the relevant information contained in the Annexes to this DPA.

13.5.4 Table 4 - neither Party has the right of termination set forth in Section 19 of the UK IDTA.

13.6 The parties agree that with respect to Swiss Personal Data the EU SCCs will apply amended and adapted as follows:

13.6.1 the Swiss Federal Data Protection and Information Commissioner is the exclusive supervisory authority;

13.6.2 the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18; and

13.6.3 references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced).

13.7 If Vendor receives legal process requiring disclosure of Customer Personal Data to a public authority in a Third Country that does not benefit from an adequacy decision, Vendor shall promptly, as applicable, and as permitted by applicable law: (i) inform the relevant public authority of the incompatibility of the legal process with the safeguards provided under this DPA, and the resulting conflict of obligations for Vendor; (ii) promptly notify Customer of the legal process; (iii) refrain from disclosing the Customer Personal Data until required to do so under the applicable procedural rules; and (iv) provide the minimum amount of Customer Personal Data permissible when responding to the legal process, based on a reasonable interpretation thereof.

14. General Terms

Governing law and jurisdiction

14.1 Without prejudice to clause 17 (Governing law) of the Standard Contractual Clauses:

14.1.1 the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

14.1.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

14.2 Nothing in this DPA reduces Vendor's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14.3 Subject to section 14.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

Changes in Data Protection Laws, etc.

14.4 Customer may:

14.4.1 by at least 30 (thirty) calendar days' written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 13.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

14.4.2 propose any other variations to this DPA which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.

14.5 If Customer gives notice under section 14.4.1:

14.5.1 Vendor shall promptly co-operate to ensure that equivalent variations are made to any agreement between the parties; and

14.5.2 Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Vendor to protect against additional risks associated with the variations made under section 14.4.1 and/or 14.5.1.

14.6 If Customer gives notice under section 14.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

14.7 Neither Customer nor Vendor shall require the consent or approval of any Affiliate to amend this DPA pursuant to this section 14.5 or otherwise.

Severance

14.8 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

15. **Indemnification**

16. Vendor's limitations of, and exclusions from, liability are as set forth in the Principal Agreement; provided that Vendor shall not be liable for costs or damages incurred by Customer as a result of an action or inaction by Customer that causes or results in a Security Incident.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

Customer:

Signature _____

Name _____

Title _____

Date Signed _____

Vendor: PerformYard, Inc.

Signature DocuSigned by: Sean Dunn FC665D425448406...

Name Sean Dunn

Title CEO

Date Signed Feb-05-2026 | 12:27 PM EST

APPENDIX

ANNEX 1 – DESCRIPTION OF THE PROCESSING

A. LIST OF PARTIES

Data exporter(s):

1)	**Name:**	Customer and its Affiliates
	Address:	Customer's address, as provided in the Principal Agreement
	Contact person's name, position, and contact details:	Customer's contact
	Activities relevant to the data transferred under these Clauses:	Use of Vendor's Services as described in the Agreement.
	Role (controller/processor):	Controller

Signature _____

Date Signed _____

Data importer(s):

1)	**Name:**	PerformYard, Inc.
	Address:	4201 Wilson Blvd #110420, Arlington, VA 22203
	Contact person's name, position, and contact details:	Sean Dunn, CEO 703-783-1315 / Sdunn@performyard.com
	Activities relevant to the data transferred under these Clauses:	Providing and supporting the Services as described in the Principal Agreement.
	Role (controller/processor):	Processor

Signature DocuSigned by: Sean Dunn FC665D425448406...

Date Signed Feb-05-2026 | 12:27 PM EST

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred / processed

- Data subjects include employees of the data exporter about whom data has been provided to PerformYard via the Services by (or at the direction of) the data exporter.

Categories of personal data transferred / processed

- Data exporter may provide personal information such as full name, work email address, title and manager, as well as other personal information regarding employees of data exporter to

enable performance management of employees, which may include performance reviews, goals, feedback, to-do action items, electronic documents and document signing/acknowledgment.

Special categories of data (if appropriate)

- Any special categories of data are determined and controlled by the data exporter at their sole discretion but are not required for the delivery of the Services.

Frequency of transfer

- Continuous

Nature of the processing

- The provision of Services by PerformYard under the Principal Agreement to the Customer

Purpose(s) of the data transfer and further processing

- As necessary to provide the Services according to the Principal Agreement, as specified in an Order Form, or as instructed by Customer in its use of the services.

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

- For the duration of the Services under the Principal Agreement, subject to the Deletion or Return of Customer Personal Data section.

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

- The subject matter and duration of the processing is as outlined above within this Annex. The nature of the specific subprocessing services is as relevant to the services provided by each Subprocessor.

C. COMPETENT SUPERVISORY AUTHORITY

- The competent supervisory authority is as determined in accordance with Clause 13 of the Standard Contractual Clauses.

ANNEX 2 - TECHNICAL AND ORGANISATIONAL MEASURES

PerformYard currently observes the security practices described in this Annex 2. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, PerformYard may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in this DPA.

Access Control

1. Preventing Unauthorized Product Access

Outsourced processing: PerformYard hosts its Service with outsourced cloud infrastructure providers. Additionally, PerformYard maintains contractual relationships with vendors to provide the Service in accordance with this DPA. PerformYard relies on contractual agreements, privacy policies, and vendor compliance programs to protect data processed or stored by these vendors.

Physical and environmental security: PerformYard hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: PerformYard implemented a uniform password policy for its service. Customers who interact with the service via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in PerformYard's service is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

2. Preventing Unauthorized Product Use

PerformYard implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: PerformYard implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in PerformYard's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: PerformYard maintains relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

3. Limitations of Privilege & Authorization Requirements

Product access: A subset of PerformYard's employees have access to the services and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Employees are granted access by role, and reviews of high-risk privilege grants are performed periodically. Employee roles are reviewed at least once every six months.

Background checks: All PerformYard employees undergo a background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

Transmission Control

In-transit: PerformYard makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. PerformYard HTTPS implementation uses industry standard algorithms and certificates.

At-rest: PerformYard stores user passwords following policies that follow industry standard practices for security. PerformYard has implemented technologies to ensure that stored data is encrypted at rest.

Input Control

Detection: PerformYard designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. PerformYard personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: PerformYard maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, PerformYard will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If PerformYard becomes aware of unlawful access to Customer data stored within its products, PerformYard will: 1) notify the affected Customers of the incident; 2) provide a description of the steps PerformYard is taking to resolve the incident; and 3) provide status updates to the Customer contact, as PerformYard deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form PerformYard selects, which may include via email or telephone.

Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power and network.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

PerformYard's service is designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists PerformYard operations in maintaining and updating the product applications and backend while limiting downtime.

Subprocessors

PerformYard contractually requires its Subprocessors take substantially similar measures described in this Annex 2.