

# DATA PROCESSING ADDENDUM

Last Modified: 3 May 2026

This Data Processing Addendum, including its Annexes and the Standard Contractual Clauses (“DPA”), forms an integral part of the Digital Event Passport Terms of Service, or any other written agreement that governs Customer’s use of the Digital Event Passport Services (the “Agreement”), entered into between **Digital Event Passport LLC (“Digital Event Passport”)** and the legal entity or individual that creates an account for, or otherwise accesses or uses, the Digital Event Passport Services and accepts the Agreement (“**Customer**”), and applies solely to the extent that Digital Event Passport processes any Customer Personal Data (as defined below) in connection with the Digital Event Passport Services. This DPA is effective as of the date Customer first accepts the Agreement, whether by creating an account, clicking to accept the Agreement, or using the Digital Event Passport Services. This DPA is legally binding upon acceptance of the Agreement; however, parties may execute a signed version for record-keeping purposes.

By entering into the Agreement, Customer enters into this DPA on behalf of itself and, if applicable and to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. For the purposes of the DPA only, and except where otherwise indicated, the term “**Customer**” shall include Customer and its Authorized Affiliates.

## 1. DEFINITIONS

- 1.1. “**Applicable Data Protection Laws**” means all data protection and privacy laws and regulations applicable to the respective party in its role in the processing of Customer Personal Data under the Agreement, which may include, to the extent applicable, European Data Protection Laws and the CCPA.
- 1.2. “**Authorized Affiliate**” means a Customer Affiliate who is authorized to use the Digital Event Passport Services under the Agreement and who has not signed their own separate “Agreement” with Digital Event Passport.
- 1.3. “**CCPA**” means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, et seq.), as may be amended, superseded or replaced from time to time.
- 1.4. “**Content**” means, if not defined within the Agreement, all data processed by Digital Event passport on your behalf in the course of providing the Digital Event Passport Services.
- 1.5. “**Customer Personal Data**” means any ‘personal data’ or ‘personal information’ contained within Content.
- 1.6. “**Digital Event Passport Services**” means the proprietary, cloud-based software platform and related services provided by Digital Event Passport, which enable Customers to configure and operate digital event passports, check-ins, activities, and related event engagement features for in-person, hybrid, or virtual events.

- 1.7. **“European Data Protection Laws”** means (a) Regulation 2016/679 (General Data Protection Regulation) (**“EU GDPR”**); (b) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (**“UK GDPR”**); and (c) the Swiss Federal Data Protection Act and its implementing regulations (**“Swiss Data Protection Act”**); in each case as may be amended, superseded or replaced from time to time.
  - 1.8. **“Restricted Transfer”** means a transfer (directly or via onward transfer) of personal data that is subject to European Data Protection Laws to a third country outside the European Economic Area, United Kingdom and Switzerland which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).
  - 1.9. **“Security Addendum”** means the security addendum found at Annex C.
  - 1.10. **“Security Breach”** means a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
  - 1.11. **“Standard Contractual Clauses”** or **“SCCs”** means the standard contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded or replaced from time to time.
  - 1.12. **“Subprocessor”** means any other processor engaged by Digital Event Passport to process Customer Personal Data.
  - 1.13. **“UK Addendum”** means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioners Office under S.119 (a) of the UK Data Protection Act 2018, as updated or amended from time to time.
  - 1.14. The terms **“controller”**, **“data subject”**, **“supervisory authority”**, **“processor”**, **“process”**, **“processing”**, **“personal data”**, and **“personal information”** shall have the meanings given to them in Applicable Data Protection Laws. The term **“controller”** includes **“business”**, the term **“data subject”** includes **“consumers”**, and the term **“processor”** includes **“service provider”** (in each case, as defined by the CCPA).
2. **PROCESSING OF PERSONAL DATA**
    - 2.1. **Scope and Roles of the Parties.** This DPA applies when Customer Personal Data is processed by Digital Event Passport as a processor in its provision of the Digital Event Passport Services to Customer, who will act as either a controller or processor, as applicable, of Customer Personal Data.
    - 2.2. **Customer Processing.** Customer agrees that (i) it will comply with its obligations under Applicable Data Protection Laws in its processing of Customer Personal Data and any processing instructions it issues to Digital Event Passport, and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Applicable Data Protection Laws for Digital Event Passport to process Customer Personal Data and provide the Digital Event Passport Services pursuant to the Agreement (including this DPA).
    - 2.3. **Digital Event Passport Processing.** Digital Event Passport agrees that (a) when Digital Event Passport processes Customer Personal Data in its capacity

as a processor on behalf of the Customer, Digital Event Passport will (i) comply with Applicable Data Protection Laws, and (ii) process the Customer Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with Customer's documented instructions (as set forth in the Agreement, in this DPA, or as directed by the Customer or Customer's Authorized Users through the Digital Event Passport Services). Digital Event Passport is not responsible for determining if Customer's processing instructions are compliant with applicable law. Customer acknowledges that Customer Personal Data may be processed on an automated basis as a result of Customer's configuration and use of the Digital Event Passport Services. Digital Event Passport does not monitor or review Customer Personal Data except as necessary to provide the Services, maintain security, prevent abuse, or comply with applicable law.

2.4. **Details of Processing.** The details of the processing of Customer Personal Data by Digital Event Passport are set out in Annex A to the DPA.

### 3. CONFIDENTIALITY

3.1. **Personnel.** Digital Event Passport shall ensure that any employees or personnel it authorizes to process Customer Personal Data is subject to an appropriate duty of confidentiality.

### 4. SUBPROCESSING

4.1. **Authorization.** Customer provides a general authorization to Digital Event Passport use of Subprocessors to process Customer Personal Data in accordance with this Section, including those Subprocessors listed in the Subprocessor List.

4.2. **Subprocessor Obligations.** Digital Event Passport shall (i) enter into a written agreement with its Subprocessors, which includes data protection and security measures no less protective than the measures set forth in this DPA; and (ii) remain fully liable for any breach of the Agreement and this DPA that is caused by an act, error or omission of its Subprocessors to the extent that Digital Event Passport would have been liable for such act, error or omission had it been caused by Digital Event Passport.

4.3. **Subprocessor Changes.** At least thirty (30) calendar days prior to the date on which any new Subprocessor shall commence processing Customer Personal Data, Digital Event Passport shall update the Subprocessor List and provide Customer with notice of that update. Such notice will be sent to individuals who have signed up to receive updates to the Subprocessor List via the mechanism(s) indicated on the Subprocessor List.

4.4. **Subprocessor Objections.** Customer may object to Digital Event Passport's appointment of a new Subprocessor on reasonable grounds relating to data protection by notifying Digital Event Passport in writing at [privacy@digitaleventpassport.com](mailto:privacy@digitaleventpassport.com) within ten (10) calendar days after receiving notice pursuant to Section 4.3. In such an event, Digital Event Passport and Customer will discuss those objections in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, within ten (10)

calendar days from Digital Event Passport's written notification, Customer, as its sole and exclusive remedy, may terminate the Order Form(s) with respect to only those aspects which cannot be provided by Digital Event Passport without the use of the new Subprocessor. Digital Event Passport will provide Customer with a pro rata reimbursement of any prepaid, but unused fees of such Order Form(s) following the effective date of such termination.

## 5. ASSISTANCE

5.1. **Data Subject Requests.** Customer is responsible for responding to and complying with data subject requests ("DSR"). The Digital Event Passport Services include controls that Customer may use to assist it to respond to DSR. If Customer is unable to access or delete any Customer Personal Data using such controls, Digital Event Passport shall, taking into account the nature of the processing, reasonably cooperate with Customer to enable Customer to respond to the DSR. If a data subject sends a DSR to Digital Event Passport directly and where Customer is identified or identifiable from the request, Digital Event Passport will promptly forward such DSR to Customer and Digital Event Passport shall not, unless legally compelled to do so, respond directly to the data subject except to refer them to the Customer to allow Customer to respond as appropriate.

5.2. **Data Protection Impact Assessments.** Digital Event Passport will provide reasonably requested information regarding the Digital Event Passport Services to Customer to carry out data protection impact assessments relating to the processing of Customer Personal Data and any related required consultation with supervisory authorities as required by Applicable Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

5.3. **Legal Requests.** If Digital Event Passport receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Customer Personal Data, Digital Event Passport will attempt to redirect the governmental body to request such Customer Personal Data directly from Customer. As part of this effort, Digital Event Passport may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Personal Data to a governmental body, Digital Event Passport will give Customer reasonable notice of the legal demand to allow Customer to seek a protective order or other appropriate remedy, unless Digital Event Passport is legally prohibited from doing so.

## 6. SECURITY

6.1. **Security Measures.** Digital Event Passport has implemented and will maintain appropriate technical and organizational security measures as set forth in Annex C ("Security Measures"). The Security Measures are subject to technical progress and development and Digital Event Passport may update the Security Measures, provided that any updates shall not materially diminish the overall security of Customer Personal Data or the Digital Event Passport Services. Digital Event Passport may make available certain security controls within the

Digital Event Passport Services that Customer may use in accordance with the Agreement.

- 6.2. **Security Breach Notification.** In the event of a Security Breach, Digital Event Passport will (a) notify Customer in writing without undue delay after becoming aware of the Security Breach; and (b) promptly take reasonable steps to contain, investigate, and mitigate any adverse effects resulting from the Security Breach. Digital Event Passport will reasonably cooperate with and assist Customer with respect to any required notification to supervisory authorities or data subjects (as applicable), taking into account the nature of the processing, the information available to Digital Event Passport, and any restrictions on disclosing the information (such as confidentiality).

## 7. AUDITS AND RECORDS

- 7.1. **Audit.** Digital Event Passport shall make available to Customer information reasonably necessary to demonstrate compliance with this DPA, including summaries of independent third-party audits or certifications where available. Where required by Applicable Data Protection Laws, Customer may conduct an audit or inspection of Digital Event Passport's processing of Customer Personal Data, provided that: (a) such audit is limited to matters reasonably necessary to verify compliance with this DPA; (b) Customer provides at least thirty (30) days' prior written notice; (c) the audit is conducted during normal business hours and in a manner that does not unreasonably interfere with Digital Event Passport's business operations; (d) the audit occurs no more than once in any twelve (12) month period, unless required by a supervisory authority; (e) the audit is subject to reasonable confidentiality obligations; and (f) Customer bears all costs and expenses of the audit, unless the audit reveals material non-compliance with this DPA. Customer acknowledges that the Digital Event Passport Services are hosted by Subprocessors that maintain independently validated security and compliance programs, and that audits shall not include access to such Subprocessors' systems beyond documentation made available by Digital Event Passport.

## 8. TRANSFER OF PERSONAL DATA

- 8.1. **Restricted Transfers.** Where the transfer of Customer Personal Data to Digital Event Passport is a Restricted Transfer, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form an integral part of the Agreement in accordance with Annex B of this DPA.
- 8.2. **Alternative Transfer Mechanisms.** If and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Customer Personal Data to Digital Event Passport, the parties shall reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Customer Personal Data. Additionally, in the event Digital Event Passport adopts an alternative transfer mechanism (including any successor version of the Privacy Shield), such alternative transfer

mechanism shall apply instead of the SCCs described in Section 8.1 of this DPA (but only to the extent such alternative transfer mechanism complies with applicable European Data Protection Laws and extends to the territories to which Customer Personal Data is transferred).

9. **BACKUP, DELETION & RETURN**

9.1. **No Backups.** The Digital Event Passport Services do not include customer-accessible backup services or disaster recovery for Customer Personal Data. Digital Event Passport does provide functionality within the Digital Event Passport Services that may permit Customer to backup certain Customer Personal Data on its own. It is the Customer's obligation to backup any Customer Personal Data if desired.

9.2. **Deletion.** The Digital Event Passport Services include controls that Customer may use at any time during the term of the Agreement to retrieve or delete Customer Personal Data. Subject to the terms of the Agreement, Digital Event Passport will delete Customer Personal Data from the Digital Event Passport Services when Customer uses such controls to send an instruction to delete.

9.3. **Termination.** Upon termination or expiration of the Agreement and following Customer's written request, Digital Event Passport will delete or assist Customer in deleting any Customer Personal Data within its possession or control within thirty (30) days following such request.

10. **CCPA COMPLIANCE**

10.1. Digital Event Passport shall not process, retain, use, or disclose Customer Personal Data for any purpose other than for the purposes set out in the Agreement, DPA and as permitted under the CCPA. Digital Event Passport shall not sell or share information as those terms are defined under the CCPA.

11. **GENERAL**

11.1. The parties agree that this DPA shall replace any existing data processing addendum, attachment, exhibit or standard contractual clauses that the parties may have previously entered into in connection with the Digital Event Passport Services. Digital Event Passport may update this DPA from time to time, with such updated version posted to <https://digitaleventpassport.com/dpa.pdf> or a successor website designated by Digital Event Passport; provided, however, that no such update shall materially diminish the privacy or security of Customer Personal Data. This DPA is legally binding upon acceptance of the Agreement; however, parties may execute a signed version for record-keeping purposes

11.2. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

11.3. Digital Event Passport's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions: (a) Customer is solely responsible for communicating any additional processing instructions on behalf of its Authorized Affiliates; (b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations under this DPA; and (c) if an Authorized Affiliate seeks to assert a legal demand, action, suit, claim,

proceeding or otherwise against Digital Event Passport (“Authorized Affiliate Claim”), Customer must bring such Authorized Affiliate Claim directly against Digital Event Passport on behalf of such Authorized Affiliate, unless Applicable Data Protection Laws require the Authorized Affiliate be a party to such claim, and all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability. In no event will this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.

- 11.4. In the event of any conflict between this DPA and any data privacy provisions set out in any agreements between the parties relating to the Digital Event Passport Services, the parties agree that the terms of this DPA shall prevail, provided that if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses control and take precedence. If there is any conflict between this DPA and a Business Associate Agreement entered into between the parties (“BAA”), then the BAA shall prevail to the extent of any conflict solely with respect to any PHI (as defined in such BAA).
- 11.5. Notwithstanding anything to the contrary in the Agreement or this DPA and to the maximum extent permitted by law, each party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this DPA (including all Annexes hereto), the SCCs or any data protection agreements in connection with the Agreement (if any), whether in contract, tort or under any other theory of liability, shall remain subject to the limitation of liability section of the Agreement and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA, including all Annexes hereto. Customer agrees that any regulatory penalties incurred by Digital Event Passport that arise in connection with Customer’s failure to comply with its obligations under this DPA or any laws or regulations including Applicable Data Protection Laws shall reduce Digital Event Passport’s liability under the Agreement as if such penalties were liabilities to Customer under the Agreement.
- 11.6. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.
- 11.7. The obligations placed upon each party under this DPA and the Standard Contractual Clauses shall survive so long as Digital Event Passport processes Customer Personal Data on behalf of Customer.

This DPA is legally binding upon Customer's acceptance of the Agreement (as defined in the preamble). The signature block below is provided for Customers who require a signed version for their own internal compliance or record-keeping purposes. By signing and returning this document, the Customer reaffirms its agreement to these terms.

Customer Legal Name: \_\_\_\_\_

Customer Address: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Representative Name: \_\_\_\_\_

Representative Position: \_\_\_\_\_

Date: \_\_\_\_\_

Signature for and on behalf of the Customer: \_\_\_\_\_

# ANNEX A

## DESCRIPTION OF THE PROCESSING / TRANSFER

ANNEX 1(A): LIST OF PARTIES	
Data exporter	<p>Name of the data exporter: The entity identified as the “Customer” in the Agreement and this DPA.</p> <p>Contact person’s name, position and contact details: The address and contact details associated with Customer’s Digital Event Passport account, or as otherwise specified in this DPA or the Agreement.</p> <p>Activities relevant to the data transferred: The activities specified in Annex 1(B)below.</p> <p>Signature and date: This DPA is incorporated into and accepted as part of the Agreement in accordance with its terms.</p> <p>Role (Controller/Processor): Controller (for Module 2) or Processor (for Module 3).</p>
Data importer	<p>Name of the data importer: Digital Event Passport LLC</p> <p>Contact person’s name, position and contact details: Jonathan May, Founder jonathan@digitaleventpassport.com</p> <p>Activities relevant to the data transferred: The activities specified in Annex 1.B below.</p> <p>Signature and date: This DPA is incorporated into and accepted as part of the Agreement in accordance with its terms.</p> <p>Role (Controller/Processor): Processor</p>

<p><b>ANNEX 1(B): DESCRIPTION OF THE PROCESSING / TRANSFER</b></p>	
<p>Categories of data subjects whose personal data is transferred:</p>	<p>Data subjects include individuals about whom data is provided to Digital Event Passport via the Digital Event Passport Services (by or at the direction of Customer), which shall include:</p> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <p>IF CUSTOMER HAS NOT FILLED OUT THE ABOVE SECTION:  Customer shall be deemed to have declared that the categories of data subjects include: (a) individual contacts, prospects, customers, business partners and vendors of Customer (who are natural persons); (b) employees or contact persons of Customer’s prospects, customers, business partners and vendors; (c) employees, agents, advisors, freelancers of Customer (who are natural persons); (d) Customer’s Authorized Users or (e) other individuals whose personal data is included in Content.</p>
<p>Categories of personal data transferred:</p>	<p>The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:</p> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <p>IF CUSTOMER HAS NOT FILLED OUT THE ABOVE SECTION:  Customer shall be deemed to have declared that the types of Customer Personal Data may include but are not limited to the following types of Customer Personal Data: (a) name, address, title, contact details; and/or (b) any other personal data processed in the course of the Services as Content.</p>

<p>Sensitive data transferred (if appropriate)</p>	<p>Subject to any applicable restrictions and/or conditions in the Agreement and this DPA, Customer may include 'special categories of personal data' or similarly sensitive personal data (as described or defined in Applicable Data Protection Laws) in Customer Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, at their sole risk, and which may include, but is not limited to Customer Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health and/or data concerning a natural person's sex life or sexual orientation.</p>
<p>Frequency of the Transfer</p>	<p>Continuous or one-off depending on the services being provided by Digital Event Passport.</p>
<p>Nature, subject matter and duration of the processing:</p>	<p>Nature: Digital Event Passport provides a cloud-based unified data analytics platform and related services, as further described in the Agreement.</p> <p>Subject Matter: Customer Personal Data.</p> <p>Duration: The duration of the processing will be for the term of the Agreement and any period after the termination or expiry of the Agreement during which Digital Event Passport processes Customer Personal Data.</p>
<p>Purpose(s) of the data transfer and further processing:</p>	<p>Digital Event Passport shall process Customer Personal Data for the following purposes:</p> <p>(a) as necessary for the performance of the Digital Event Passport Services and Digital Event Passport's obligations under the Agreement (including the DPA), including processing initiated by Authorized Users in their use and configuration of the Digital Event Passport Services; and (b) further documented, reasonable instructions from Customer agreed upon by the parties (the "Purposes").</p>
<p>Period for which the personal data will be retained:</p>	<p>Digital Event passport will retain Customer Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Digital Event Passport processes Customer Personal Data in accordance with the Agreement.</p>

ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY

Competent supervisory authority

The data exporter's competent supervisory authority will be determined in accordance with the EU GDPR.

# ANNEX B

## STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)

1. Subject to Section 8.1 of the DPA, where the transfer of Customer Personal Data to Digital Event Passport is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form part of the DPA as follows:

a. In relation to transfers of Customer Personal Data protected by the EU GDPR, the SCCs shall apply as follows:

1. Module Two terms shall apply (where Customer is the controller of Customer Personal Data) and the Module Three terms shall apply (where Customer is the processor of Customer Personal Data);
2. in Clause 7, the optional docking clause shall apply and Authorized Affiliates may accede the SCCs under the same terms and conditions as Customer, subject to mutual agreement of the parties;
3. in Clause 9, option 2 (“general authorization”) is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in Section 4.3 of the DPA;
4. in Clause 11, the optional language shall not apply;
5. in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;
6. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
7. Annex I shall be deemed completed with the information set out in Annex A to the DPA; and
8. Annex II shall be deemed completed with the information set out in the Security Addendum, subject to Section 6.1 (Security Measures) of the DPA.

b. In relation to transfers of Customer Personal Data protected by the UK GDPR, the SCCs as implemented under Section 1(a) above shall apply with the following modifications:

1. the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;
2. Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex A and Annex B to the DPA and the Security Addendum respectively, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting “neither party”; and
3. Any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

c. In relation to transfers of Customer Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1(a) above will apply with the following modifications:

1. references to “Regulation (EU) 2016/679” and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

2. references to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to “Switzerland” and/or “Swiss law” (as applicable);
3. references to the “competent supervisory authority” and “competent courts” shall be replaced with references to the “Swiss Federal Data Protection Information Commissioner” and “applicable courts of Switzerland”);
4. the SCCs shall be governed by the laws of Switzerland ; and
5. disputes shall be resolved before the competent Swiss courts.

2. Where the Standard Contractual Clauses apply pursuant to Section 8.1 of this DPA, this section sets out the parties’ interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a party complies with the interpretations set out below, that party shall be deemed by the other party to have complied with its commitments under the Standard Contractual Clauses:

1. where Customer is itself a processor of Customer Personal Data acting on behalf of a third party controller and Digital Event Passport would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), Digital Event Passport may interact solely with Customer and Customer shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;
2. the certification of deletion described in Clause 16(d) of the SCCs shall be provided by Digital Event Passport to Customer upon Customer’s written request;
3. for the purposes of Clause 15(1)(a) the SCCs, Digital Event Passport shall notify Customer and not the relevant data subject(s) in case of government access requests, and Customer shall be solely responsible for notifying the relevant data subjects as necessary; and
4. Taking into account the nature of the processing, Customer agrees that it is unlikely that Digital Event Passport would become aware of Customer Personal Data processed by Digital Event Passport is inaccurate or outdated. To the extent Digital Event Passport becomes aware of such inaccurate or outdated data, Digital Event Passport will inform the Customer in accordance with Clause 8.4 SCCs.

# Annex C

## Security Measures

We currently observe the Security Measures described in this Annex C. All capitalized terms not otherwise defined herein will have the meanings as set forth in the Agreement.

### a) Access Control

#### i) Preventing Unauthorized Product Access

**Outsourced processing:** We host our Service on outsourced cloud infrastructure providers, according to a shared responsibility model. Additionally, we maintain contractual relationships with vendors in order to provide the Services in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

**Physical and environmental security:** We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers.

**Authentication:** We implement an email-based one-time passcode access policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing Customer Data.

**Authorization:** Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products 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.

**Application Programming Interface (API) access:** Public product APIs can be accessed using an API key.

#### ii) Preventing Unauthorized Use

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

**Intrusion detection and prevention:** We implement 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: Code stored in our source code repositories is checked for best practices and identifiable software flaws using automated tooling.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” (JITA) requests for access; all such requests are logged. Employees are granted access by role.

b) Transmission Control

In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We never knowingly store plaintext passwords; if necessary, we store hashed, salted results of authentication material, as appropriate for the use-case.

c) Input Control

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

Response and tracking: We maintain 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, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure uptime.

Fault tolerance: Backup strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer Data is stored in cold storage (S3 for AWS).

Online replicas and backups: All databases are backed up and maintained using at least industry standard methods.

The server instances that support the products are architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

# Subprocessor List

To receive notifications about updates to this list of Subprocessors, email your request to [privacy@digitaleventpassport.com](mailto:privacy@digitaleventpassport.com).

<b>Name of Sub-processor</b>	<b>Description of Processing</b>
Amazon Web Services, Inc	Infrastructure, hosting, and database services
Cloudflare, Inc.	File storage, DNS, content delivery, caching, security, and related infrastructure services
Crisp IM	Customer support and chat services
Microsoft Corporation	Usage analytics and performance monitoring services
Neon, LLC	Managed database hosting services
Statsig, LLC	Feature flagging and experimentation services
Stripe, Inc.	Payment processing, billing, invoicing, fraud prevention
Supabase, Inc.	Infrastructure, storage, authentication, and database services
Vercel Inc.	Infrastructure, hosting, and database services