PARTIES AND EXECUTION

Entity details: Obrecsys 3349 Hwy 138 Wall, NJ 07719 USA	Entity details: **[INSERT COUNTERPARTY]**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

VARIABLES

Parties' relationship	Controller to Processor – Business to Service Provider	
Parties' roles	You will act as the Controller and Business (as defined in Section 1 of the Terms). Obrecsys LLC. will act as the Processor and Service Provider (as defined in Section 1 of the Terms).	
Contacts	Processor	Controller
	Name: Email: [INSERT ADDITIONAL DETAILS]	Name: Email: [INSERT ADDITIONAL DETAILS]
Main Agreement	Terms And Conditions - Managers and Team Members – https://docs.kampfire.events/TC_Ma.pdf	
Term	This DPA will commence on the final date of signature and will have the same duration as, and will be subject to, the termination terms of the Main Agreement	
Breach Notification Period	Without Undue Delay after becoming aware of a personal data breach.	
Sub-processor Notification Period	A reasonable timeframe before the new sub-processor is granted access to Personal Data.	
Liability Cap	Each party's aggregate liability under this DPA will not exceed the liability caps as per the Main Agreement.	
Governing Law and Jurisdiction	The governing law clause of the Main Agreement shall also apply to this DPA	
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data, including in the European Economic Area (EEA), the United Kingdom (UK), the United States of America (USA) and Other Jurisdictions	

VARIABLES	
	or Locations. This includes the: European Union Regulation (EU) 2016/679 UK addendum in accordance with section 119A(1) of the Data Protection Act 2018 California Consumer Privacy Act of 2018 (**CCPA**)/California Privacy Rights Act of 2020 (**CPRA**) each as amended from time to time.
Services related to processing	As described in the Main Agreement
Duration of processing	For the Term of this DPA, subject to a maximum retention of three (3) years per event from the date the event was created in the Platforms. Following deletion (whether by automatic expiration, Controller action, or Audience erasure request), residual copies in encrypted backups are permanently destroyed within thirty-five (35) days. Encrypted, pseudonymized affiliate and coupon records may be retained for up to seven (7) years for tax, accounting, audit and other legal-compliance purposes.
Nature and purpose of processing	Provide you with the access to the Platforms, its content and Our Services, and any other information, products or services that you request from Us. Pair Audience Information with biometric data and other metadata information derived from photos, as part of Our core Services. Identify your Audience in photos taken at events or for marketing campaigns and which are uploaded to Our Services, using facial recognition software, which is provided by AWS, in order to create grouped personalized albums. Facial recognition is used by Us to analyze photos uploaded to the Platforms and to identify if a user appears in any of such uploaded photos. The Managers, then have the option to group such photos and send to Audience the specific photos in which they appear. The facial recognition is governed by AWS's privacy policy. Fulfil any other purpose for which you provided it. If you create an account, register for Our newsletter or otherwise approve communications with us, to give you notices about your account, including expiration and renewal notices. Carry out Our obligations and enforce Our rights arising from any contracts entered into between you and us, including for billing and collection. Notify you when Our Platforms are available, and of changes to any products or services We offer or provide through it. Request feedback and to contact you about your use of Our Platforms and Services. Keep Our Platforms, you and the Audience safe and secure (for example, for fraud monitoring and prevention).
Personal Data	name, email address, image and photos, location data, contact information, including country of residence, payment information, and social media login data
Data subjects	You and your Audience (as defined in the Main Agreement)

VARIABLES

Special provisions	
Transfer Mechanism	If you are a resident of the European Economic Area, please be advised that all transfers to the USA are based on the European Commission's Standard Contractual Clauses. If you are a resident of the United Kingdom, we rely on the UK Addendum to the Standard Contractual Clauses (approved by the UK authorities) For all such transfers based on Standard Contractual Clauses or the UK Addendum to the Standard Contractual Clauses, We also whenever necessary, have implemented similar appropriate safeguards with Our third-party service providers and partners. The Standard Contractual Clauses can be found at https://docs.kampfire.events/SCC_TOMS_Ma.pdf

ANNEX 1

Security measures. Technical and organisational measures to ensure the security of Personal Data	https://docs.kampfire.events/SCC_TOMS_Ma.pdf

ANNEX 2

Sub-processors. Current sub-processors	**[Insert Processor's/Sub-processor's list of sub-processors, either in full or as a link to relevant webpage]**

TERMS

This Data Processing Addendum ("**DPA**") forms part of the Main Agreement between Kampfire, operated by Obrecsys LLC. ("**Kampfire**") and Customer. This DPA reflects the parties' agreement regarding the Processing of Customer Personal Data.

If there is any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA will govern. All capitalized terms not defined herein will have the meaning set forth in the Agreement or under Privacy Laws and Regulations.

In the course of providing Kampfire's platform ("**Service**") to Customer pursuant to the Agreement, Kampfire may Process Customer Personal Data on behalf of Customer. The parties agree to comply with the following provisions with respect to Customer Personal Data Processed by Kampfire as part of the Services**.**

1. **What is this agreement about?**

2. **Purpose**. The parties are entering into this Data Processing Agreement (**DPA**) for the purpose of processing Personal Data (as defined above).

3. **Definitions.** Under this DPA:

    1. **adequate country** means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data,
    2. **Controller**, **data subject**, **personal data breach**, **process/processing**, **Processor** and **supervisory authority** have the same meanings as in the Data Protection Laws,

3. **Customer** means the entity that executed the Main Agreement and shall be deemed the "Data Controller" for the purposes of the DPA
4. **Business** and **Service Provider** have the same meanings as in the CCPA/CPRA, and
5. **Sub-Processor** means another processor engaged by the Processor to carry out specific processing activities with Personal Data.

4. **What are each party's obligations?**

5. **Controller obligations.** Controller instructs Processor to process Personal Data in accordance with this DPA, and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow Processor to process Personal Data.

6. **Processor obligations.** Processor will:

1. only process Personal Data in accordance with this DPA and Controller's instructions (unless legally required to do otherwise),
2. not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA and the Main Agreement,
3. inform Controller immediately if (in its opinion) any instructions infringe Data Protection Laws,
4. use the technical and organisational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved,
5. notify Controller of a personal data breach within the Breach Notification Period and provide assistance to Controller as required under Data Protection Laws in responding to it,
6. ensure that anyone authorised to process Personal Data is committed to confidentiality obligations,
7. without undue delay, provide Controller with reasonable assistance with:
    1. data protection impact assessments,
    2. responses to data subjects' requests to exercise their rights under Data Protection Laws, and
    3. engagement with supervisory authorities,
8. if requested, provide Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA,
9. allow for audits at Controller's reasonable request, provided that audits are limited to once a year and during business hours except in the event of a personal data breach, and
10. return Personal Data upon Controller's written request or delete Personal Data by the end of the Term, unless retention is legally required. Deletion of Personal Data is effected immediately in active systems; residual copies in encrypted backups are permanently destroyed within thirty-five (35) days. Processor also makes available to Controller in-product tooling permitting Controller to set per-event deletion dates (capped at three (3) years from event creation), to erase the Personal Data of an individual data subject ("forget guest"), and to erase the Personal Data of all data subjects of an event ("forget all guests"); and makes available to data subjects a self-service erasure mechanism ("Forget Me") within the relevant guest panel.

3. **Warranties**. The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

4. **Sub-processing**

5. **Use of sub-processors.** Controller authorises Processor to engage other processors (referred to in this section as **sub-processors**) when processing Personal Data. Processor's existing sub-processors are listed in Annex 2.

6. **Sub-processor requirements.** Processor will:

1. require its sub-processors to comply with equivalent terms as Processor's obligations in this DPA,
2. ensure appropriate safeguards are in place before internationally transferring Personal Data to its sub-processor, and
3. be liable for any acts, errors or omissions of its sub-processors as if they were a party to this DPA.

3. **Approvals.** Processor may appoint new sub-processors provided that they notify Controller in writing in accordance with the Sub-processor Notification Period.

4. **Objections.** Controller may reasonably object in writing to any future sub-processor. If the parties cannot agree on a solution within a reasonable time, either party may terminate this DPA.

5. **International personal data transfers**

6. **Instructions.** Processor will transfer Personal Data outside the UK, the EEA or an adequate country only on documented instructions from Controller, unless otherwise required by law.

7. **Transfer mechanism.** Where a party is located outside the UK, the EEA or an adequate country and receives Personal Data:

1. that party will act as the **data importer**,
2. the other party is the **data exporter**, and
3. the relevant Transfer Mechanism will apply.

3. **Additional measures.** If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.
4. **Disclosures.** Subject to terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):

1. challenge the request and promptly notify the data exporter about it, and
2. only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

5. **Other important information**

    1. **Survival.** Any provision of this DPA which is intended to survive the Term will remain in full force.
    2. **Order of precedence.** In case of a conflict between this DPA and other relevant agreements, they will take priority in this order:

1. Transfer Mechanism,
2. DPA,
3. Main Agreement.

3. **Notices.** Formal notices under this DPA must be in writing and sent to the Contact on the DPA's front page as may be updated by a party to the other in writing.
4. **Third parties.** Except for affiliates, no one other than a party to this DPA has the right to enforce any of its terms.
5. **Entire agreement.** This DPA supersedes all prior discussions and agreements and constitutes the entire agreement between the parties with respect to its subject matter and neither party has relied on any statement or representation of any person in entering into this DPA.

6. **Amendments.** Any amendments to this DPA must be agreed in writing.
7. **Assignment.** Neither party can assign this DPA to anyone else without the other party's consent.
8. **Waiver.** If a party fails to enforce a right under this DPA, that is not a waiver of that right at any time.
9. **Governing law and jurisdiction.** The Governing Law applies to this DPA and all disputes will only be litigated in the courts of the Jurisdiction.