CROSS-BORDER PERSONAL DATA TRANSFER

1. **DEFINITIONS**

Capitalized terms not defined herein will have the meaning set forth in the DPA or under Privacy Laws and Regulations.

"**Kampfire**" means Obrecsys LLC.

"**nFADP**" means the Swiss Federal Act on Data Protection of 19 June 1992 (Status as of March 1, 2019) as amended by the new Act on Federal Data Protection and the Data Protection Ordinance on September 1, 2023.

"**IDTA**" means the International Data Transfer Agreement, issued by the ICO in accordance with section 119A of the Data Protection Act 2018, or any other applicable standard contractual clauses issued, approved, or otherwise recognized by the ICO.

"**Privacy Laws and Regulations**" means: (**A**) Regulation (EU) 2016/679 ("**GDPR**"); and (**B**) the 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**").

"**Swiss SCCs**" means the applicable standard contractual clauses issued, approved, or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**").

"**Third Country**" means a country outside the European Economic Area ("**EEA**"), the UK or Switzerland, which was not acknowledged by the EU Commission, a UK Secretary of State or the FDPIC (as applicable) as providing an adequate level of protection in accordance with Article 45(3) of the GDPR, Article 45 of the UK GDPR or the equivalent.

A "**Transfer**" means a transfer by Kampfire, Kampfire's New Sub-processors or Kampfire's Sub-processors of: (**1**) GDPR-governed Customer Personal Data transferred outside the EEA ("**EEA Transferred Data**"); (**2**) UK-GDPR governed Customer Personal Data transferred outside the UK ("**UK Transferred Data**"); and, (**3**) nFADP-governed Customer Personal Data transferred outside of Switzerland ("**Swiss Transferred Data**", and with EEA and UK Transferred Data: "**Transferred Data**").

"**UK Addendum**" means the UK addendum published by the Information Commissioner's Office's ("**ICO**") in accordance with section 119A(1) of the Data Protection Act of 2018, incorporating the EU SCCs.

2. **EEA TRANSFERS**

Transfers of EEA Transferred Data to a Third Country, will be made under the EU SCCs, giving effect to module 2, which is incorporated by reference to this DPA, as follows:

In Clause 7, the optional docking clause will not apply.

If applicable - in clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes will be as set out in Section 3 of the DPA.

In clause 11, the optional language will not apply.

In clause 17, Option 1 will apply, and the EU SCCs will be governed by the Irish law.

In clause 18(b), disputes will be resolved before the courts of Ireland.

3. **UK TRANSFERS**

Transfers of UK Transferred Data to a Third Country, will be made -

In accordance with the EU SCCs as detailed in section 2 above, as amended by the UK Addendum, which is incorporated by reference to this DPA, with the necessary changes made as detailed in sections 12-15 to the UK Addendum; or,

If the EU SCCs as implemented above cannot be used to lawfully Transfer UK Transferred Data, the IDTA will instead be incorporated by reference, will form an integral part of this DPA, and will apply to Swiss Transferred Data. In such case, the relevant Annexes of the Swiss SCCs will be populated using the information contained in **ANNEXES A-B** to the DPA.

4. **SWISS TRANSFERS**

Transfers of Swiss Transferred Data to a Third Country, will be made -

In accordance with the EU SCCs as detailed in section 2 above, as recognized by the FDPIC on August 27, 2021, with the following modifications: (**A**) references to 'EU', 'Union', 'Member State' and 'Member State law' will be interpreted as references to 'Switzerland', and 'Swiss law', as applicable; and, (**B**) references to 'Competent Supervisory Authority' and 'Competent courts' will be interpreted as references to the FDIPC and Competent courts in Switzerland; or,

if the EU SCCs as implemented above cannot be used to lawfully Transfer Swiss Transferred Data in compliance with the nFADP, the Swiss SCCs will instead be incorporated by reference, will form an integral part of this DPA, and will apply to Swiss Transferred Data. In such case, the relevant Annexes of the Swiss SCCs will be populated using the information contained in **ANNEXES A-B** to the DPA.

5. **SUPPLEMENTAL MEASURES**

In accordance with Article 46 of the GDPR, the EU SCCs and guidelines published by the European Data Protection Board (EDPB), and without prejudice to any provisions of the DPA or this Annex, Kampfire undertakes to implement the following organizational and technical safeguards, in addition to the safeguards mandated by the EU SCCs, to ensure the required adequate level of protection to Transferred Data:

Technical and Organizational Measures. Kampfire will implement and maintain the technical and organizational measures, as specified in **Annex II** above, with a purpose to protect Customer Personal Data against any processing for national security or other government purposes that go beyond what is necessary and proportionate in a democratic society, considering the type of processing activities under the Main Agreement and relevant circumstances.

Contractual Measures. For the purposes of safeguarding Transferred Data when any Third Country's Supervisory Authority requests access to such data ("**Request by Supervisory Authority**"), and unless required by a valid court order or if otherwise Kampfire may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to EEA Transferred Data, or where the access is requested under Request by Supervisory Authority in the event of imminent threat to lives, Kampfire will:

- not purposefully create back doors or similar programming that could be used to access EEA Transferred Data;

- not provide the source code or encryption keys to any Supervisory Authority for the purpose of accessing EEA Transferred Data;
- upon Customer's written request, provide reasonable available information about the Request by Supervisory Authority of access to Customer Personal Data by Supervisory Authority Kampfire has received in the 6 months preceding to Customer's request; and,
- notify Customer upon receiving a Request by the Supervisory Authority to access Customer Personal Data to enable Customer to take necessary actions, communicate directly with the relevant Supervisory Authority and to respond. If Kampfire is prohibited by law to notify the Customer of such Request by Supervisory Authority, Kampfire will make reasonable efforts to challenge such prohibition through judicial action or other means at Customer's expense and, to the extent possible, will provide only the minimum amount of information necessary.

6. **FUTURE ADEQUACY**

As applicable, if: (**A**) the Adequacy Recognition is invalidated or otherwise terminated by the EU Commission or a UK Secretary of State; (**B**) the EU SCCs are invalidated or are no longer in effect; or (**C**) any other Transfer safeguard used for the Transfer of Transferred Data is no longer in effect for any reason, then Kampfire will take such alternative lawful measures, as may be available and applicable, to continue facilitating the lawful Transfer of Transferred Data by Kampfire, Kampfire's Sub-processors, Kampfire' New Sub-processors, or equivalents thereof.

Annex I to the EU SCCs
- DETAILS OF THE PERSONAL DATA PROCESSING -

1. **LIST OF PARTIES**

Data exporter

Name, address and contact details: Customer, whose name, address, and contact details are as detailed under the Main Agreement.

Activities relevant to the data transferred under these Clauses: Provision of Services under the Agreement.

Signature and date: The data exporter's signature on the DPA or agreement between the parties applies herein.

Role (controller/processor): Controller.

Data importer

Name: Obrecsys LLC. ("**Kampfire**")

Address: 3349 Hwy 138 Wall NJ, 07719 USA.

Contact person's name, position and contact details: Bikash Chapagain, email address: security@kampfire.events.

Activities relevant to the data transferred under these Clauses: Provision of services under the Main Agreement.

Signature and date: The data importer's signature on the DPA or agreement between the parties, applies herein.

Role (controller/processor): Processor

2. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

- Audience of the events and campaigns.
- Events and campaigns managers using the Services.

Categories of personal data transferred

- Credentials and Account Data.
- Photos, Text and Documents.
- Biometric data and other metadata information derived from photos.

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

- Biometric data and other metadata information derived from photos.

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

Continuous and subject to the Main Agreement.

Nature of the processing

Provision of the services under the agreement between the parties.

Purpose(s) of the data transfer and further processing

Provision of the services under the Main Agreement.

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

Duration of the Main Agreement, subject to a maximum retention of three (3) years per event from the date the event was created in the Platforms. Following deletion, residual copies in encrypted backups are permanently destroyed within thirty-five (35) days.

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

Hosting and ancillary services for the duration of the Main Agreement.

3. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13:

Where the data exporter is established in an EU Member State - the Supervisory Authority of such EU Member State shall act as competent Supervisory Authority

Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) - the Supervisory Authority of the Member State in which the representative is established shall act as competent Supervisory Authority.

Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) - the Supervisory Authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent Supervisory Authority.

Annex II to the EU SCCs
- TECHNICAL AND ORGANIZATIONAL MEASURES -

Technical and Organizational Measures to Ensure the Security of The Data

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

MEASURE	DESCRIPTION
Measures of pseudonymization and encryption of personal data	Pseudonymization of personal data of data subjects where possible. Application of security controls, e.g., data siloing, restricting and monitoring access, designating confidential status, employing best-practice technologies.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Development and implementation of technologies and systems that accord with industry standards. Evaluation and monitoring of security of each important third-party partner during initiation of and periodically over the life of its relationship with Kampfire.
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	Development and implementation of response plans for incidents of concern, which permit investigation, mitigation and notification. Such plans are organized according to security risk and include internal and external messaging protocols.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Performance of periodic reviews by privacy, security and engineering teams to ensure all measures align with best industry practices.
Measures for user identification and authorization	Development and implementation of procedures to authenticate and respond to DSARs and to limit systems access to authorized individuals.

MEASURE	DESCRIPTION
Measures for the protection of data during storage	Pseudonymization and minimization of personal data of data subjects where possible; storage of data only so long as needed and in accordance with agreed-upon timeframes and in accordance with legal requirement
Measures for ensuring physical security of locations at which personal data are processed	Restriction of access to storage facilities on need-to-know basis; implementation of access and security controls in accordance with industry standards; training of all relevant personnel regarding security and protection of data.
Measures for ensuring system configuration, including default configuration	Implementation of configuration management tools where appropriate.
Measures for internal IT and IT security governance and management	Appointment of persons responsible for maintaining security management and data protection.
Measures for certification/assurance of processes and products	Implementation of relevant controls and processes.
Measures for ensuring data minimization	Pseudonymization and minimization of personal data of data subjects where possible; storage of data only so long as needed and in accordance with agreed-upon timeframes; limitation to data necessary to perform the services
Measures for ensuring limited data retention	Implementation and periodic review of data retention and destruction policies and procedures. Automated enforcement of a three (3) year per-event retention cap for photos, derived metadata and biometric templates, with a thirty-five (35) day backup-purge window following deletion.
Measures for ensuring accountability	Implementation and periodic review of data mapping and data protection policies and procedures
Measures for allowing data portability and ensuring erasure	Development and implementation of procedures to authenticate and respond to DSARs. In-product self-service erasure ("Forget Me") for data subjects, and Controller-initiated erasure of individual or all data subjects of an event.